



Docket No.: K2291.0109
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Yukiyasu Tsunoo

Application No.: 10/669,269

Filed: September 25, 2003

Art Unit: Not Yet Assigned

For: DATA ENCRYPTION SYSTEM AND
METHOD

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

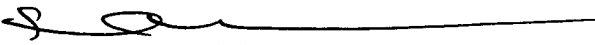
Applicant hereby claims priority under 35 U.S.C. 119 based on the following
prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Japan	2002-280469	September 26, 2002

In support of this claim, a certified copy of the said original foreign application is
filed herewith.

Dated: October 17, 2003

Respectfully submitted,

By 
Steven I. Weisburd
Registration No.: 27,409
DICKSTEIN SHAPIRO MORIN &
OSHINSKY LLP
1177 Avenue of the Americas
41st Floor
New York, New York 10036-2714
(212) 835-1400
Attorney for Applicant

15

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 9 月 2 6 日
Date of Application:

出 願 番 号 特 願 2 0 0 2 - 2 8 0 4 6 9
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 2 8 0 4 6 9]

出 願 人 日 本 電 気 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 8 月 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 6 3 9 1 2

【書類名】 特許願

【整理番号】 35001172

【提出日】 平成14年 9月26日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 角尾 幸保

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088959

 【弁理士】

 【氏名又は名称】 境 廣巳

【手数料の表示】

 【予納台帳番号】 009715

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9002136

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号装置及び暗号プログラム

【特許請求の範囲】

【請求項 1】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号文の暗号処理または復号処理における前記変換表に対するアクセス時のキャッシュミスヒット回数を、任意の平文または暗号文についてはほぼ均一化する調整手段を備えたことを特徴とする暗号装置。

【請求項 2】 前記調整手段は、暗号処理または復号処理で使用する複数の変換表のうち攻撃対象とされる可能性の高いものとして設定された変換表のみを調整対象とすることを特徴とする請求項 1 記載の暗号装置。

【請求項 3】 攻撃対象とされる可能性の高い変換表には、エントリ総数に対する参照総エントリ数の比である利用率が小さな変換表を含むことを特徴とする請求項 2 記載の暗号装置。

【請求項 4】 前記調整手段は、前記変換表をキャッシュにプリロードする手段を備えることを特徴とする請求項 1、2 または 3 記載の暗号装置。

【請求項 5】 前記調整手段は、キャッシュミスヒット回数が増加する方向に調整することを特徴とする請求項 1、2 または 3 記載の暗号装置。

【請求項 6】 前記調整手段は、変換表のエントリのうち暗号処理または復号処理で実際に使用されたエントリを管理する使用エントリ管理手段と、変換表のエントリのうち暗号処理または復号処理で実際に使用されなかったエントリをアクセスする不使用エントリロード手段とを備えたことを特徴とする請求項 5 記載の暗号装置。

【請求項 7】 前記調整手段は、変換表のエントリのうち暗号処理または復号処理で実際に使用されたエントリを管理する使用エントリ管理手段と、変換表の使用エントリの最大数と暗号処理または復号処理で実際に使用されたエントリ数の差分だけキャッシュミスヒットを発生させるキャッシュミスヒット発生手段とを備えたことを特徴とする請求項 5 記載の暗号装置。

【請求項 8】 前記調整手段は、暗号処理または復号処理で変換表のエン

りにキャッシュヒットした回数を管理する使用エントリ管理手段と、前記キャッシュヒットした回数だけキャッシュミスヒットを発生させるキャッシュミスヒット発生手段とを備えたことを特徴とする請求項 5 記載の暗号装置。

【請求項 9】 前記調整手段は、暗号処理または復号処理で変換表のエントリにキャッシュヒットする毎にキャッシュミスヒットを発生させる手段を備えたことを特徴とする請求項 5 記載の暗号装置。

【請求項 10】 前記調整手段は、1つの平文または1つの暗号文の暗号処理または復号処理で参照される総回数が n 回である同一内容の変換表を n 個備え、各参照毎にそれぞれ異なる変換表を参照させるものであることを特徴とする請求項 5 記載の暗号装置。

【請求項 11】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号文の暗号処理または復号処理における暗号処理時間または復号処理時間を、任意の平文または暗号文についてほぼ均一化する調整手段を備えたことを特徴とする暗号装置。

【請求項 12】 前記調整手段は、実質的な暗号処理または復号処理に要した時間を計測する計測手段と、計測された時間が予め設定された時間より短い場合、不足している時間だけ暗号処理または復号処理に要する時間を延長する延長手段とを含むことを特徴とする請求項 11 記載の暗号装置。

【請求項 13】 前記予め設定された時間として、実質的な暗号処理または復号処理に要する最大時間を用いたことを特徴とする請求項 12 記載の暗号装置。

【請求項 14】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号文の実質的な暗号処理または復号処理に要した時間を計測する計測手段と、計測された時間が予め設定された時間より短い場合、予め設定された一定時間または無作為に決定した時間だけ暗号処理または復号処理に要する時間を常に或いは無作為に延長する延長手段とを含む調整手段を備えたことを特徴とする暗号装置。

【請求項 15】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号文の暗号処理または復号処理に要する時間を調整する調整手段を備え、該調整手段は、予め設定された一定時間または無作為に決定した時間だけ暗号処理または復号処理に要する時間を常に或いは無作為に延長する延長手段を含むことを特徴とする暗号装置。

【請求項 16】 換字処理を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、換字処理に用いる変換表のうち攻撃対象とされる可能性の高い変換表でない場合にはテーブル構造の変換表として備え、攻撃対象とされる可能性の高い変換表の場合はテーブル構造の変換表として持たずに演算処理によって換字処理を実行することを特徴とする暗号装置。

【請求項 17】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムであって、キャッシュ装備のコンピュータで実行されたときに1つの平文または1つの暗号文の暗号処理または復号処理における前記変換表に対するアクセス時のキャッシュミスヒット回数を、任意の平文または暗号文についてはほぼ均一化する調整手段を有することを特徴とする暗号プログラム。

【請求項 18】 前記調整手段は、暗号処理または復号処理で使用する複数の変換表のうち攻撃対象とされる可能性の高いものとして設定された変換表のみを調整対象とすることを特徴とする請求項 17 記載の暗号プログラム。

【請求項 19】 攻撃対象とされる可能性の高い変換表には、エントリ総数に対する参照総エントリ数の比である利用率が小さな変換表を含むことを特徴とする請求項 18 記載の暗号プログラム。

【請求項 20】 前記調整手段は、前記変換表をキャッシュにプリロードする手段を備えることを特徴とする請求項 17、18 または 19 記載の暗号プログラム。

【請求項 21】 前記調整手段は、キャッシュミスヒット回数が増加する方向に調整することを特徴とする請求項 17、18 または 19 記載の暗号プログラ

ム。

【請求項 2 2】 前記調整手段は、変換表のエントリのうち暗号処理または復号処理で実際に使用されたエントリを管理する使用エントリ管理手段と、変換表のエントリのうち暗号処理または復号処理で実際に使用されなかったエントリをアクセスする不使用エントリロード手段とを備えたことを特徴とする請求項 2 1 記載の暗号プログラム。

【請求項 2 3】 前記調整手段は、変換表のエントリのうち暗号処理または復号処理で実際に使用されたエントリを管理する使用エントリ管理手段と、変換表の使用エントリの最大数と暗号処理または復号処理で実際に使用されたエントリ数の差分だけキャッシュミスヒットを発生させるキャッシュミスヒット発生手段とを備えたことを特徴とする請求項 2 1 記載の暗号プログラム。

【請求項 2 4】 前記調整手段は、暗号処理または復号処理で変換表のエントリにキャッシュヒットした回数を管理する使用エントリ管理手段と、前記キャッシュヒットした回数だけキャッシュミスヒットを発生させるキャッシュミスヒット発生手段とを備えたことを特徴とする請求項 2 1 記載の暗号プログラム。

【請求項 2 5】 前記調整手段は、暗号処理または復号処理で変換表のエントリにキャッシュヒットする毎にキャッシュミスヒットを発生させる手段を備えたことを特徴とする請求項 2 1 記載の暗号プログラム。

【請求項 2 6】 前記調整手段は、1つの平文または1つの暗号文の暗号処理または復号処理で参照される総回数がn回である同一内容の変換表をn個備え、各参照毎にそれぞれ異なる変換表を参照させるものであることを特徴とする請求項 2 1 記載の暗号プログラム。

【請求項 2 7】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムであって、キャッシュ装置のコンピュータ上で実行されたときに1つの平文または1つの暗号文の暗号処理または復号処理における暗号処理時間または復号処理時間を、任意の平文または暗号文についてほぼ均一化する調整手段を有することを特徴とする暗号プログラム。

【請求項 2 8】 前記調整手段は、実質的な暗号処理または復号処理に要した時間を計測する計測手段と、計測された時間が予め設定された時間より短い場

合、不足している時間だけ暗号処理または復号処理に要する時間を延長する延長手段とを含むことを特徴とする請求項 2 7 記載の暗号プログラム。

【請求項 2 9】 前記予め設定された時間として、実質的な暗号処理または復号処理に要する最大時間を用いたことを特徴とする請求項 2 8 記載の暗号プログラム。

【請求項 3 0】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムであって、1つの平文または1つの暗号文の実質的な暗号処理または復号処理に要した時間を計測する計測手段と、計測された時間が予め設定された時間より短い場合、予め設定された一定時間または無作為に決定した時間だけ暗号処理または復号処理に要する時間を常に或いは無作為に延長する延長手段とを含む調整手段を有することを特徴とする暗号プログラム。

【請求項 3 1】 ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムであって、1つの平文または1つの暗号文の暗号処理または復号処理に要する時間を調整する調整手段を備え、該調整手段は、予め設定された一定時間または無作為に決定した時間だけ暗号処理または復号処理に要する時間を常に或いは無作為に延長する延長手段を含むことを特徴とする暗号プログラム。

【請求項 3 2】 換字処理を用いて暗号処理または復号処理を行う暗号プログラムであって、換字処理に用いる変換表のうち攻撃対象とされる可能性の高い変換表でない場合にはテーブル構造の変換表として備え、攻撃対象とされる可能性の高い変換表である場合はテーブル構造の変換表として持たずに演算処理によって換字処理を実行することを特徴とする暗号プログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明はデータの通信や蓄積の際にデータを秘匿するための暗号装置に関し、特に換字テーブルなどの変換表を用いてデータを暗号化する暗号装置の改良に関する。

【0 0 0 2】

【従来の技術】

一般に暗号方式は、共通鍵暗号と公開鍵暗号に大別される。共通鍵暗号では、暗号化アルゴリズムは公開するが、暗号化の鍵と復号化の鍵が同一であり、鍵の値を秘密にする。他方、公開鍵暗号は、暗号化の鍵と復号化の鍵が異なり、暗号化アルゴリズムに加えて暗号化の鍵を公開し、復号化の鍵を秘密にする。公開鍵暗号は、鍵の配送の手間がかからず鍵管理が容易である等の利点を有するが、共通鍵暗号に比べて処理量が多くなり処理速度が遅くなるといった問題があるため、大量データの暗号化には共通鍵暗号が専ら使用されている。

【0 0 0 3】

共通鍵暗号は、更に、ブロック暗号とストリーム暗号とに分けられる。ストリーム暗号は、乱数生成器が出力する乱数列を1ビットずつデータに作用させるビット単位の処理によって暗号化する。他方、ブロック暗号は、数十ビット以上の比較的長いデータブロック毎に暗号化および復号化を行う。ブロック暗号の代表的なものに、DES暗号、FEAL暗号などがある。

【0 0 0 4】

DES暗号やFEAL暗号などの暗号処理部は、データランダム化部と鍵生成部とで構成される。鍵生成部は、鍵を拡大し、データランダム化部に出力する。データランダム化部は、平文（または暗号文）と鍵を混ぜ合わせ、暗号文（または平文）を出力する。データランダム化部は、通常、入力部、データ変換部および出力部で構成される。入力部は、初期置換（IP：Initial Permutation）など簡単な処理を行い、出力部は逆初期置換（ IP^{-1} ）などの処理を行う。データ変換部は、入力部の出力と鍵生成部で生成された鍵とを用いて、基本的な単位操作を複数回繰り返し、結果を出力部へ出力する。単位操作では、排他的論理和、換字（substitution）、置換（coordinate permutation）などの操作が組み合わされる。

【0 0 0 5】

換字の処理を行う部分は、Sボックスとも呼ばれる。Sボックスでは、一般に換字テーブルと呼ばれる変換表が使われ、Sボックスの入力ビット列で表される番地に格納されているビット列を換字テーブルから読み出し、Sボックスの出力と

して出力する。一般に S ボックスは、使用する換字テーブルの種類に応じて複数種類存在し、入力ビット数に応じて S 7 ボックス、S 9 ボックスなどとして区別される。各 S i ボックスは、一般に 1 ブロックの暗号化（または復号）の過程で複数回実行される。

【0 0 0 6】

図 1 3 に換字テーブルの簡単な例を示す。この例の換字テーブルは 1 6 個のエントリを有し、各エントリに 1 6 進数で 0 から F の番地が振られており、各エントリに 0 から F の値が格納されている。左上のエントリを 0 番地とし、右方向に 1、2、3 番地を割振り、2 段目は左から右に 4、5、6、7 番地を、3 段目は同じく左から右に 8、9、A、B 番地を、4 段目は同じく左から右に C、D、E、F 番地を割振るものとする、例えば、入力ビットが 0 0 0 0（1 6 進数で 0）の場合、0 番地のエントリに格納されている 1 6 進数で 8 の値が読み出され、2 進数で表現した 1 0 0 0 が出力される。このような換字テーブルを使用すると、換字テーブルを交換するだけで異なる暗号変換を実施でき、秘匿通信の柔軟性が向上する等の利点がある。

【0 0 0 7】

図 1 4 は従来の暗号装置のブロック図である。図 1 4 において、1 は CPU（演算装置）、2 はメモリ（主記憶）、3 は暗号プログラム、4 はキャッシュであり、CPU 1 とキャッシュ 4 との間はデータ線、アドレス線および制御線を含むプロセッサバス 5 によって接続され、キャッシュ 4 とメモリ 2 との間は、同じくデータ線、アドレス線および制御線を含むメモリバス 6 によって接続されている。周知のようにキャッシュ 4 は、メモリ 2 よりも高速アクセス可能な小容量のメモリであり、メモリ 2 の内容の一部の写しを保持する。CPU 1 がプロセッサバス 5 を通じて要求する命令やデータがキャッシュ 4 に存在すれば（これをキャッシュヒットと呼ぶ）、キャッシュ 4 はキャッシュヒットした命令やデータを直ちに CPU 1 に返却する。他方、CPU 1 が要求する命令やデータがキャッシュ 4 に存在しなければ（これをキャッシュミスヒットと呼ぶ）、キャッシュ 4 はミスヒットした命令やデータを含む所定サイズのデータをメモリバス 6 を通じてメモリ 2 から読み出して自身に格納すると共に CPU 1 に該当する命令やデータを返却

する。ここで、所定サイズのデータとは、例えば 3 2 バイト、1 2 8 バイトといったサイズである。このようなサイズでキャッシュ 4 に読み込んでおくことにより、命令が実行される場合には実行アドレスが近い命令が続けて実行されることが多いという原理（命令の局所性の原理）により、キャッシュヒット率を高めることができ、高速化が可能となる。

【 0 0 0 8 】

暗号プログラム 3 は、前述した D E S 暗号や F E A L 暗号などの共通鍵暗号を実現するプログラムであり、通常は図示しない磁気ディスク等の補助記憶装置に格納されており、使用時に図 1 4 に示すようにメモリ 2 にロードされて実行される。図 1 4 のメモリ 2 のブロックの右に記載した構成図は、1 つの平文を暗号化する際の暗号プログラム 3 の処理の内容を示している。

【 0 0 0 9 】

暗号プログラム 3 は、他のプログラムからの呼出しなどによって起動されると（ステップ 3 0 1）、先ず、入力部 3 0 2 によって、平文の入力、初期置換などの処理を行い、その後、鍵生成部 3 0 3 による鍵生成処理、データ変換部 3 0 4 によるデータ変換処理が実行される。鍵生成部 3 0 3 では、暗号プログラム 3 に設定されている鍵を拡大し、データ変換部 3 0 4 で使う幾つかの鍵（拡大鍵）を生成する。拡大鍵は、共通鍵が変更されなければ変化せず、平文や暗号文に依存しない。そのため、鍵生成部 3 0 3 をあらかじめ一度実行して拡大鍵を生成記憶し、暗号化／復号化では記憶した拡大鍵を使い、鍵生成部 3 0 3 を動作させない場合もある。データ変換部 3 0 4 は、入力部 3 0 2 から出力された初期置換後の平文と鍵生成部 3 0 3 で生成された鍵を混ぜ合わせる基本操作を複数回繰り返し、結果のデータを出力する。このとき、換字を行う場合は、暗号プログラム 3 に予め設定されている換字テーブル 3 0 5 をアクセスして換字処理が実行される。データ変換部 3 0 4 で複数回の基本操作が繰り返されて得られたデータは、出力部 3 0 6 において逆初期置換などの処理が実行され、最終的に得られた暗号文が呼出し元のプログラム等に返却され、1 つの平文の暗号化を終える（ステップ 3 0 7）。復号処理は、暗号化の逆となり、ほぼ同様の動作となる。

【 0 0 1 0 】

一方、暗号アルゴリズムで使われる鍵を解読する方法が幾つか存在する。古典的な解読方法は、鍵の全数探索法と呼ばれるもので、鍵の値として取りうる全ての値を用いて既知の平文の暗号化を試み、既知の暗号文と一致するかどうかを調べるものである。しかし、この方法は鍵長が長くなると調べるべき鍵の候補数が膨大となり、現実的でなくなる。このため、調べるべき鍵の候補数を現実的な範囲に押え込む解読方法として、差分解読法や線形解読法が提案されている。更に近年においては、主に公開鍵暗号を対象としたタイミングアタックと呼ばれる方法が提案され（後述する非特許文献1参照）、更にタイミングアタックに対する防御技術が提案されている（後述する特許文献1参照）。

【0011】

非特許文献1に記載されるタイミングアタックは、公開鍵暗号の基本演算である冪乗剰余演算の演算時間の差違に基づいて秘密鍵の候補を絞り込むものであり、このため特許文献1では、冪乗剰余演算毎に伝搬遅延によるクリティカルパスの遅延時間を変化させることで、公開鍵暗号に対するタイミングアタックを防御している。

【0012】

【非特許文献1】

Paul C.Kohcer, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Advances in Cryptology: Proceedings of Crypto 96, Plenum Press, 1995, pp104-113

【特許文献1】

特開平10-222065号公報

【0013】

【発明が解決しようとする課題】

本発明者は、換字テーブルを用いて暗号化を行う図14に示したような暗号装置の安全性を研究する過程で、新たな暗号解読法を見出した。以下、この新たな暗号解読法をキャッシュ攻撃型暗号解読法と呼び、その解読方法について説明する

。

【 0 0 1 4 】

今、図 1 5 に示すように、平文 P_0 と鍵 k_0 の排他的論理和で換字テーブル S を引いた出力値と、平文 P_1 と鍵 k_1 の排他的論理和で同じ換字テーブル S を引いた出力値とを暗号文とする暗号器を考えてみる。そして、双方で換字テーブル S のそれぞれ異なるエントリを引いたものとする。このとき、次式が成り立つ。

$$P_0 \circ k_0 \neq P_1 \circ k_1$$

$$P_0 \circ P_1 \neq k_0 \circ k_1 = \Delta k$$

… (1)

ここで、記号 \circ は排他的論理和を示し、鍵 k_0 、 k_1 のビット数は n である。また、 Δk を鍵差分と呼ぶ。

【 0 0 1 5 】

式 (1) は 2 テーブルモデルであるが、一般に n テーブルモデルへ拡張することができ、次式が導き出せる。

$$P_i \circ k_i \neq P_j \circ k_j$$

$$P_i \circ P_j \neq k_i \circ k_j = \Delta k_{ij}$$

… (2)

ここで、 $i, j = 1 \sim n$ である。

【 0 0 1 6 】

式 (2) は、暗号過程（または復号過程）で換字テーブル S を n 回引く場面がある場合に、全ての場面で換字テーブル S の異なるエントリを引くこととなる任意の 2 つの平文 P_i と平文 P_j の排他的論理和は鍵差分 Δk_{ij} に一致せず、且つ、任意の 2 つの鍵はその鍵差分が Δk_{ij} となる関係にあることを意味する。このような鍵差分 Δk_{ij} が求まれば、鍵探索の範囲は 2^{2N} から 2^N に狭まる。例えば、図 1 5 において $k_0 \circ k_1 = \Delta k$ の N ビットが求まれば、 k_0 の N ビットを全数探査すれば $k_1 = k_0 \circ \Delta k$ で他方の N ビットの k_1 が計算できるからである。これにより、 k_0 と k_1 の $2N$ ビットの全数探査が、 k_0 のみの N ビットの全数探査で済むようになる。

【 0 0 1 7 】

鍵差分 Δk_{ij} は、例えば以下のようにして求めることができる。先ず、図 16 (a) に示すように、鍵差分 Δk_{ij} の取りうる全ての値毎に初期値として値 0 のカウンタを設定したテーブルを用意する。次に、暗号過程の全場面で換字テーブル S の異なるエントリを引く多数の平文の集合から任意のペアを抽出し、そのペアの排他的論理和の値と一致する鍵差分 Δk_{ij} に対応するカウンタを +1 する処理を、全てのペアについて繰り返す。この結果、カウンタの値は図 16 (b) に示すように更新されていき、初期値 0 のまま或いは極めて小さな値（この値は式 (2) の成立確率に依存する）になっているカウンタに対応する鍵差分 Δk_{ij} の値が求める鍵差分となる。

【0018】

次に、暗号過程（または復号過程）で換字テーブル S を n 回引く場面がある場合に、全ての場面（もしくは、かなり多くの場面）で換字テーブル S の異なるエントリを引くこととなる任意の平文の集合を求める方法について説明する。

【0019】

図 14 で説明したように、キャッシュ 4 を備えるコンピュータで暗号プログラム 3 を実行すると、CPU 1 の処理速度が一定で、他のプログラムが実行されていない理想的な環境下でも、与える平文（または暗号文）によって暗号化処理時間（または復号時間）が相違する。その理由は、与える平文が異なれば、換字テーブル (S) 305 の使用するエントリが異なる場合があり、換字テーブル 305 アクセス時のキャッシュヒット率が相違するからである。つまり、キャッシュミスヒットが最も多くなる平文の暗号処理時間が最も長くなる。キャッシュミスヒットが最も多くなる平文は、換字テーブル S を引く全場面（もしくは、かなり多くの場面）で異なるエントリを引いている可能性があるとして推測される。

【0020】

本発明者は、この推測の正しさを、既知の暗号アルゴリズムを用いて検証した。検証に使用した暗号アルゴリズムは、1996 年に三菱電気株式会社によって提案された MISTY1 という、64 ビットのブロック暗号（鍵長は 128 ビット）である。図 17 に MISTY1 のデータランダム化部の構成を示し、図 18 にデータランダム化部で使用される FO 関数と、さらにこの FO 関数で使用さ

れる $F I i j$ 関数の構成を示す。 $F O i$ 関数は合計 8 個あり、1 つの $F O i$ 関数の中に 3 個の $F I i j$ 関数があり、1 つの $F I i j$ 関数の中で換字テーブル S 9 が 2 回使用され、換字テーブル S 7 が 1 回使用されている。つまり、暗号化の過程で、換字テーブル S 9 は、 $8 \times 3 \times 2 = 48$ 回使用され、換字テーブル S 7 は $8 \times 3 \times 1 = 24$ 回使用される。換字テーブル S 9 は入力が 9 ビットで、512 のエントリ（サンプルプログラムでは 1 エントリのサイズは 32 ビットで記述されていた）を有し、換字テーブル S 7 は入力が 7 ビットで、128 のエントリ（サンプルプログラムでは 1 エントリのサイズは 8 ビットで記述されていた）を有する。

【0021】

図 19 は、MISTY1 で多数の平文を暗号化したときの暗号化時間の分布を示し、横軸は暗号化時間、縦軸は平文数である。また、図 20 は、暗号化時間と変換テーブル S 9 の動作エントリ数の関係を示し、図 21 は、暗号化時間と変換テーブル S 7 の動作エントリ数の関係を示す。ここで、動作エントリ数とは、変換テーブルのエントリの内、幾つのエントリが暗号化処理で使用されたかを示し、変換テーブル S 9 の最大値は 48、変換テーブル S 7 の最大値は 24 である。図 19 および図 20 から理解されるように、暗号処理時間が或るしきい値 T 以上かかる平文は、換字テーブル S 9 を引く殆どの場面で異なるエントリを引いており、毎回キャッシュミスヒットを起こしているために暗号処理時間が長くなっている。これに対し、変換テーブル S 7 は、動作エントリ数にかかわらず暗号処理時間はほぼ一定である。変換テーブル S 9 と S 7 とでこのような差違が生じる理由は、変換テーブル S 7 は 128 エントリと小型のテーブルであるため、何回かミスヒットするとキャッシュ 4 にテーブルの大部分のエントリがロードされて、その後ミスヒットが発生しなくなるのに対し、変換テーブル S 9 は 512 エントリと大型のテーブルであるため、そのような状況が発生しないためと考えられる。従って、図 15 および図 16 で説明した原理による攻撃は、換字テーブル S 7 に対しては余り効果がなく、換字テーブル S 9 が攻撃対象となる。

【0022】

図 22 は、暗号過程で換字テーブル S 9 をほぼ 48 回引く可能性が高い平文の集

合を抽出する処理の一例を示す。まず、MISTY1の暗号プログラムをコンピュータのメモリにロードする（ステップ101）。次に、乱数によって平文を生成し（ステップ102）、コンピュータのキャッシュをクリアし（ステップ103）、前記生成した平文を暗号化対象の平文に設定して（ステップ104）、MISTY1による暗号化とこの暗号化の処理に要した時間の測定とを行う（ステップ105）。次に、測定した暗号化時間が予め設定したしきい値T以上であるかどうかを判定する（ステップ106）。ここで、しきい値Tは図19および図20のTで示される暗号化時間を使用する。しきい値Tは、解読が成立するのに必要十分な数の平文が得られるように設定する。因みに、式（2）の成立確率が高いほど少ない数の平文で足りる。そして、暗号化時間がしきい値T以上であれば、今回の平文を保存し（ステップ107）、ステップ102に戻って上述した処理を繰り返す。暗号化時間がしきい値T以上でなければ、今回の平文を保存せずにステップ102に戻って上述した処理を繰り返す。このような処理の繰り返しのによって、暗号過程で換字テーブルS9をほぼ48回引く可能性が高い平文を十分な数だけ抽出することができる。

【0023】

こうして抽出した平文の集合を用いて、図16で示したような方法で鍵差分 Δk を決定し、鍵の候補を絞り込む。そして、最終的には、確定しなかった鍵のビット部分について総当りによってビット値を確定することにより、秘密鍵の全ビットを特定する。

【0024】

このように、キャッシュを備えるコンピュータに、換字テーブルを用いて暗号化処理を行う暗号プログラムを実装した暗号装置では、キャッシュ攻撃型暗号解読法により、暗号化時間から換字エントリの動作エントリ数が推測され、鍵差分の決定によって鍵の候補数が絞り込まれ、最終的には鍵の全ビットが解読されてしまう危険性がある。キャッシュ攻撃型暗号解読法はタイミングアタックの一種と考えられるが、冪乗剰余積演算を使用しない共通鍵暗号に対して適用されるため、特許文献1記載の技術では防御できない。このため、キャッシュ攻撃型暗号解読方法に頑健な暗号装置の開発が強く望まれる。

【0025】

本発明はこのような事情に鑑みて提案されたものであり、その目的は、キャッシュ攻撃型暗号解読法に対する防御機能を備えた暗号装置を提供することにある。

【0026】**【課題を解決するための手段】**

第1の観点に基づく本発明の暗号装置は、ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号文の暗号処理または復号処理における前記変換表に対するアクセス時のキャッシュミスヒット回数を、任意の平文または暗号文についてはほぼ均一化する調整手段を備えたことを特徴とする。ここで、前記調整手段は、暗号処理または復号処理で使用する複数の変換表のうち攻撃対象とされる可能性の高いものとして設定された変換表のみを調整対象として良い。また、攻撃対象とされる可能性の高い変換表には、エントリ総数に対する参照総エントリ数（動作エントリ数）の比である利用率が小さな変換表を含むようにして良い。

【0027】

前記調整手段は、実質的な暗号処理または復号処理におけるキャッシュミスヒット回数が減少するように、前記変換表をキャッシュにプリロードする手段を備えるようにして良い。

【0028】

また前記調整手段は、キャッシュミスヒット回数が増加する方向に調整するようにして良い。この場合、前記調整手段は、変換表のエントリのうち暗号処理または復号処理で実際に使用されたエントリを管理する使用エントリ管理手段と、変換表のエントリのうち暗号処理または復号処理で実際に使用されなかったエントリをアクセスする不使用エントリロード手段とを備えるようにしても良いし、変換表のエントリのうち暗号処理または復号処理で実際に使用されたエントリを管理する使用エントリ管理手段と、変換表の使用エントリの最大数と暗号処理または復号処理で実際に使用されたエントリ数の差分だけキャッシュミスヒットを発生させるキャッシュミスヒット発生手段とを備えるようにしても良い。また、暗

号処理または復号処理で変換表のエントリにキャッシュヒットした回数を管理する使用エントリ管理手段と、前記キャッシュヒットした回数だけキャッシュミスヒットを発生させるキャッシュミスヒット発生手段とを備えるようにしても良いし、暗号処理または復号処理で変換表のエントリにキャッシュヒットする毎にキャッシュミスヒットを発生させる手段を備えるようにしても良い。更に、1つの平文または1つの暗号文の暗号処理または復号処理で参照される総回数が n 回である同一内容の変換表を n 個備え、各参照毎にそれぞれ異なる変換表を参照させるものであっても良い。

【0029】

第2の観点に基づく本発明の暗号装置は、ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号文の暗号処理または復号処理における暗号処理時間または復号処理時間を、任意の平文または暗号文についてはほぼ均一化する調整手段を備えたことを特徴とする。この場合、前記調整手段は、実質的な暗号処理または復号処理に要した時間を計測する計測手段と、計測された時間が予め設定された時間より短い場合、不足している時間だけ暗号処理または復号処理に要する時間を延長する延長手段とを含むものであっても良い。また、前記予め設定された時間として、実質的な暗号処理または復号処理に要する最大時間を用いても良い。

【0030】

第3の観点に基づく本発明の暗号装置は、ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号文の実質的な暗号処理または復号処理に要した時間を計測する計測手段と、計測された時間が予め設定された時間より短い場合、予め設定された一定時間または無作為に決定した時間だけ暗号処理または復号処理に要する時間を常に或いは無作為に延長する延長手段とを含む調整手段を備えたことを特徴とする。また、ビット列変換に使用する変換表を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、1つの平文または1つの暗号

文の暗号処理または復号処理に要する時間を調整する調整手段を備え、該調整手段は、予め設定された一定時間または無作為に決定した時間だけ暗号処理または復号処理に要する時間を常に或いは無作為に延長する延長手段を含むことを特徴とする。

【0 0 3 1】

第4の観点に基づく本発明の暗号装置は、換字処理を用いて暗号処理または復号処理を行う暗号プログラムをキャッシュ装備のコンピュータに実装した暗号装置において、換字処理に用いる変換表のうち攻撃対象とされる可能性の高い変換表でない場合にはテーブル構造の変換表として備え、攻撃対象とされる可能性の高い変換表である場合はテーブル構造の変換表として持たずに演算処理によって換字処理を実行することを特徴とする。

【0 0 3 2】

【作用】

第1の観点に基づく本発明の暗号装置にあっては、1つの平文または1つの暗号文の暗号処理または復号処理における換字テーブル等の変換表に対するアクセス時のキャッシュミスヒット回数が、任意の平文または暗号文についてほぼ均一化されるため、換字テーブル等の変換表の動作エントリ数が少ない平文または暗号文も、反対に多い平文または暗号文も、その暗号時間または復号時間がほぼ同じになり、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。このため鍵差分を決定できず、鍵の解読が困難となる。

【0 0 3 3】

第2の観点に基づく本発明の暗号装置にあっては、1つの平文または1つの暗号文の暗号処理または復号処理における暗号処理時間または復号処理時間が任意の平文または暗号文について均一化されるため、換字テーブル等の変換表の動作エントリ数が少ない平文または暗号文も、反対に多い平文または暗号文も、その暗号時間または復号時間がほぼ同じになり、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。このため鍵差分を決定できず、鍵の解読が困難となる。

【0 0 3 4】

第 3 の観点に基づく本発明の暗号装置にあっては、真に最大暗号時間を与える平文とそれ以外の平文の一部とが同じ暗号時間および復号時間になり、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【 0 0 3 5 】

第 4 の観点に基づく本発明の暗号装置にあっては、キャッシュ型攻撃暗号解読法による攻撃の可能性の高い換字テーブルが無いので、それに対するキャッシュミスはそもそも発生せず、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【 0 0 3 6 】

【発明の第 1 の実施の形態】

図 1 を参照すると、本発明の第 1 の実施の形態にかかる暗号装置は、ハードウェアとして CPU 1 とメモリ（主記憶） 3 とキャッシュ 4 とを含んで構成されるコンピュータ上に暗号プログラム 3 A が実装されている。

【 0 0 3 7 】

CPU 1 とキャッシュ 4 との間はデータ線、アドレス線および制御線を含むプロセッサバス 5 によって接続され、キャッシュ 4 とメモリ 2 との間は、同じくデータ線、アドレス線および制御線を含むメモリバス 6 によって接続されている。キャッシュ 4 は、メモリ 2 よりも高速アクセス可能な小容量のメモリであり、メモリ 2 の内容の一部の写しを保持する。CPU 1 がプロセッサバス 5 を通じて要求する命令やデータがキャッシュ 4 に存在すれば、キャッシュヒットした命令やデータがキャッシュ 4 から直ちに CPU 1 に返却される。他方、CPU 1 が要求する命令やデータがキャッシュ 4 に存在しなければ、キャッシュ 4 はミスヒットした命令やデータを含む所定サイズのデータをメモリバス 6 を通じてメモリ 2 から読み出して自身に格納すると共に CPU 1 に該当する命令やデータを返却する。前記所定サイズとしては、例えば 3 2 バイト、1 2 8 バイトが使用される。

【 0 0 3 8 】

暗号プログラム 3 A は、DES 暗号や FEAL 暗号など、ビット列変換に使用す

る変換表を用いて暗号処理または復号処理を行う共通鍵暗号を実現するプログラムであり、通常は図示しない磁気ディスク等の補助記憶装置に格納されており、使用時に図1に示すようにメモリ2にロードされて実行される。図1のメモリ2のブロックの右に記載した構成図は、1つの平文を暗号化する際の暗号プログラム3Aの処理の内容を示している。ここで、プリロード部311が調整手段を構成する。

【0039】

暗号プログラム3Aは、他のプログラムからの呼出しなどによって起動されると（ステップ301）、先ず、入力部302によって、平文の入力、初期置換などの処理を行う。次いで、本実施の形態の特徴として、プリロード部311によって、ビット列変換に使用する変換表である換字テーブル305をキャッシュ4にプリロードする処理を行う（ステップ311）。このプリロードは、例えば、換字テーブル305の全エントリを一度リードする処理で可能である。このプリロード処理時に発生するキャッシュミスヒット回数をC回とする。このキャッシュミスヒット回数Cは、任意の平文および暗号文について等しい。

【0040】

プリロード対象とする換字テーブル305は、本実施の形態の場合、暗号処理または復号処理で使用する全ての換字テーブルのうち、キャッシュ攻撃暗号解読法で攻撃される可能性の高い換字テーブルである。攻撃対象とされる可能性の高い換字テーブルは、当該暗号プログラムのアルゴリズムに照らして事前に決定され、暗号プログラム3Aに設定されている。図17および図18で説明したMISTY1の場合、変換テーブルS9が設定される。一般的に、図20で示されるように、暗号時間が長くなるのに応じて動作エントリ数が増加する傾向を示す換字テーブルが攻撃対象とされる可能性が高い。また、簡便な方法として、エントリ総数に対する参照総エントリ数（動作エントリ数）の比である利用率が小さい変換表を、攻撃対象とされる可能性の高い換字テーブルとして決定する方法を用いることができる。

【0041】

次に、暗号プログラム3Aは、鍵生成部303による鍵生成処理、データ変換部

3 0 4 によるデータ変換処理を実行する。鍵生成部 3 0 3 では、暗号プログラム 3 A が使用する共通鍵を拡大し、データ変換部 3 0 4 で使う幾つかの鍵を生成する。データ変換部 3 0 4 は、入力部 3 0 2 から出力された初期置換後の平文と鍵生成部 3 0 3 で生成された鍵を混ぜ合わせる基本操作を複数回繰り返し、暗号文を出力する。このとき、換字を行う場合は、暗号プログラム 3 A に予め設定されている換字テーブル 3 0 5 をアクセスして換字処理が実行されるが、換字テーブルのうちプリロード部 3 1 1 でキャッシュ 4 にプリロードされた換字テーブルのアクセス時にはほぼ 1 0 0 % 近くキャッシュヒットする。換言すれば、攻撃対象となる可能性の高いものとして設定された換字テーブルに対する、実質的な暗号処理におけるキャッシュミスヒット回数はほぼ 0 に均一化される。

【 0 0 4 2 】

データ変換部 3 0 4 で複数回の基本操作が繰り返されて得られたデータは、出力部 3 0 6 において逆初期置換などの処理が実行され、最終的に得られた暗号文が呼出し元のプログラム等に返却され、1 つの平文の暗号化を終える（ステップ 3 0 7）。

【 0 0 4 3 】

以上の暗号プログラム 3 A の動作は平文を暗号化する際の動作であるが、一般に暗号処理と復号処理の大部分は同じである。概略を説明すると、まず、入力部 3 0 2 によって、暗号文の入力、初期置換などの処理を行い、次いで、プリロード部 3 1 1 によって、攻撃される可能性の高い換字テーブル 3 0 5 をキャッシュ 4 にプリロードし、鍵生成部 3 0 3 による鍵生成処理、データ変換部 3 0 4 によるデータ変換処理を実行する。鍵生成部 3 0 3 では、暗号時と逆の順番で順次に鍵を生成してデータ変換部 3 0 4 に供給し、データ変換部 3 0 4 では、暗号時と逆の順番で基本操作を複数回繰り返し、その結果を出力する。最後に出力部 3 0 6 において逆初期置換などの処理が実行され、最終的に得られた平文が呼出し元のプログラム等に返却され、1 つの暗号文の復号を終える（ステップ 3 0 7）。

【 0 0 4 4 】

本実施の形態によれば、キャッシュ型攻撃暗号解読法の攻撃対象とされる可能性の高い換字テーブルについては、1 つの平文または 1 つの暗号文の実質的な暗号

処理または復号処理におけるアクセス時のキャッシュミスヒット回数が、任意の平文または暗号文についてはほぼ0に均一化される。また、その換字テーブルのプリロード時におけるキャッシュミスヒット回数は常に一定回数Cとなる。従って、攻撃対象とされる可能性の高い換字テーブルの動作エントリ数が少ない平文または暗号文も、反対に多い平文または暗号文も、その暗号時間または復号時間がほぼ同じになり、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。そうすると、鍵差分を決定できず、結果として鍵の解読が困難となる。

【0045】

以上の説明では、キャッシュ型攻撃暗号解読法で攻撃される可能性の高い換字テーブルだけをプリロードしたが、キャッシュ4の容量が許すなら、全ての換字テーブルをプリロードするようにしても良い。この場合、真に残したい換字テーブルがキャッシュのLRU等の掃き出しアルゴリズムで掃き出されてしまわないように、攻撃される可能性の高い換字テーブルは他の換字テーブルより後にプリロードするのが望ましい。また、キャッシュ4に保持されたデータに優先度を付けることができ、優先度の高いデータほど掃き出され難くすることができるコンピュータでは、攻撃される可能性の高い換字テーブルのデータに高い優先度を設定してプリロードするのが望ましい。

【0046】

図1の実施の形態では、換字テーブル305を参照する箇所が暗号プログラム3Aのデータ変換部304内だけであるDES等の共通鍵暗号を対象としたので、換字テーブルのプリロード部311をデータ変換部304の直前に設けたが、スタートのステップ301の直後に設けるようにしても良い。こうすれば、入力部302や、鍵生成部303においても換字テーブル305を参照するような共通鍵暗号に対しても適用可能である。また、同じ換字テーブルのプリロードを複数の時点、例えばスタートのステップ301の直後とデータ変換部304の直前に設けるようにしても良い。更に、暗号プログラム3Aが呼出される前に、換字テーブル305のプリロード処理を行うプログラムを別途設けることも考えられる。

【0047】

また、図1の実施の形態では、プリロード対象となる換字テーブルの全エントリがキャッシュ4にプリロードされるようにしたが、例えば約半分程度のエントリをプリロードしても、キャッシュミスヒット回数を或る程度均一化できるため、必ずしも全エントリをプリロードする必要はない。

【0048】

【発明の第2の実施の形態】

図2(a)を参照すると、本発明の第2の実施の形態にかかる暗号装置は、図1の第1の実施の形態にかかる暗号装置と比較して、暗号プログラム3Bには、換字テーブル305のプリロード部がなく、その代わりに、換字テーブル305のエントリのうち暗号処理または復号処理で実際に使用されたエントリを管理する使用エントリ管理部312と、換字テーブル305のエントリのうち暗号処理または復号処理で実際に使用されなかったエントリをアクセスする不使用エントリロード部313とを備えている。ここで、使用エントリ管理部312と不使用エントリロード部313とで調整手段を構成する。以下、第1の実施の形態の暗号装置との相違点を中心に、本実施の形態の構成と動作を説明する。

【0049】

図2(b)は使用エントリ管理部312に備わる管理テーブルの一例を示す。この管理テーブルは、キャッシュ攻撃型暗号解読法によって攻撃される可能性の高い換字テーブル毎に対応して設けられ、対応する換字テーブルと同数のエントリを持つ。管理テーブルの各エントリは、暗号処理および復号処理の開始時点で未使用を示す値にクリアされる。図2(b)では、×の記号が未使用を示す。使用エントリ管理部312は、暗号処理または復号処理の過程で、攻撃される可能性の高い換字テーブルのエントリが参照される毎に、対応する管理テーブルの対応するエントリを使用済みを示す値に変更する。図2(b)では、○の記号が使用済みを示す。つまり、○の記号が付けられたエントリに対応する換字テーブルエントリは動作エントリであることが示される。

【0050】

不使用エントリロード部313は、実際の暗号処理または復号処理でもはや換字

テーブル 305 が参照されなくなった時点で、図 2 (b) の管理テーブルを参照し、攻撃対象とされる可能性の高い換字テーブル毎に、参照されなかったエントリの全てをロード（参照、リード）する命令を実行する。

【0051】

次に本実施の形態の効果を説明する。今、攻撃対象とされる可能性の高い換字テーブルとして、MISTY1 の換字テーブル S9 を考える。この換字テーブル S9 のエントリ総数は 512、1 文の暗号化または復号化で動作するエントリ数（最大動作エントリ数）は 48 である。図 22 で説明したように攻撃者は、暗号プログラム 3B の起動前に換字テーブル S9 をクリアするため、1 つの平文を暗号化する際の換字テーブル S9 のキャッシュミスヒット回数の最大値は 48 になる。また、実際上は出現しないかも知れないが、1 つの平文を暗号化する際の換字テーブル S9 のキャッシュミスヒット回数の最小数を 1 とする。

【0052】

キャッシュミスヒット回数が最大の 48 の場合、動作エントリ数も 48 なので、不使用エントリロード部 313 は、 $512 - 48 = 464$ エントリをリードする。このときのキャッシュミスヒット回数は、既に 48 エントリのキャッシュミスヒットにより換字エントリ S9 の未だ参照されていない他の多くのエントリがキャッシュ 4 に存在するため、「小さな数の或る回数」となる。他方、キャッシュミスヒット回数が最小の 1 の場合、動作エントリ数も 1 なので、不使用エントリロード部 313 は、 $512 - 1 = 511$ エントリをリードする。このときのキャッシュミスヒット回数は、未だ 1 エントリのキャッシュミスしか起こしていないので換字エントリ S9 の未だ参照されていない他の多くのエントリはキャッシュ 4 に存在しないため、「大きな数の或る回数」となる。従って、最終的なキャッシュミスヒット回数は、キャッシュミスヒット回数が最大の 48 の場合、 $48 +$ 「小さな数の或る回数」となり、キャッシュミスヒット回数が最小の 1 の場合、 $1 +$ 「大きな数の或る回数」となり、両者は均一化される傾向を示す。このため、第 1 の実施の形態と同様の理由で、キャッシュ攻撃型暗号解読法に対する防御が可能になる。

【0053】

以上の説明では、キャッシュ型攻撃暗号解読法で攻撃される可能性の高い換字テーブルについてだけ不使用エントリ分のロードを実行したが、全ての換字テーブルを対象にして同様のロードを実行しても良い。

【0054】

【発明の第3の実施の形態】

図3を参照すると、本発明の第3の実施の形態にかかる暗号装置は、図2(a)の第2の実施の形態にかかる暗号装置と比較して、暗号プログラム3Cに、不使用エントリロード部313の代わりに、換字テーブル305の使用エントリの最大数と暗号処理または復号処理で実際に使用されたエントリ数の差分である不足エントリ数だけキャッシュミスヒットを発生させるキャッシュミスヒット発生部314を備えている。ここで、使用エントリ管理部312とキャッシュミスヒット発生部314とで調整手段を構成する。以下、第2の実施の形態の暗号装置との相違点を中心に、本実施の形態の構成と動作を説明する。

【0055】

第2の実施の形態と同様に使用エントリ管理部312は、図2(b)に示したような管理テーブルによって、キャッシュ攻撃型暗号解読法によって攻撃される可能性の高い換字テーブル毎に、暗号処理または復号処理で実際に使用されたエントリを管理している。キャッシュミスヒット発生部314は、実際の暗号処理または復号処理でもはや換字テーブル305が参照されなくなった時点で、図2(b)の管理テーブルを参照し、攻撃対象とされる可能性の高い換字テーブル毎に、使用エントリの最大数と使用されたエントリ数の差分である不足エントリ数を算出する。そして、その不足エントリ数の総数だけ、キャッシュミスヒットを発生させる処理を実行する。この処理は、例えばメモリ2上に暗号化および復号化で使わないデータ領域を設定しておき、キャッシュ4に一度に読み込まれるデータサイズ以上の間隔でリード要求を発行することで可能である。

【0056】

次に本実施の形態の効果を説明する。今、攻撃対象とされる可能性の高い換字テーブルとして、MISTY1の換字テーブルS9を考える。この換字テーブルS9のエントリ総数は512、最大動作エントリ数は48である。図22で説明し

たように攻撃者は、暗号プログラム 3 C の起動前に換字テーブル S 9 をクリアするため、1 つの平文を暗号化する際の換字テーブル S 9 のキャッシュミスヒット回数の最大値は 48 である。また、最小数は第 2 の実施の形態と同様に 1 を想定する。

【0057】

キャッシュミスヒット回数が最大の 48 の場合、動作エントリ数も 48 なので、キャッシュミスヒット発生部 314 は、不足エントリ数として、 $48 - 48 = 0$ を算出する。従って、この場合はキャッシュミスヒットはもはや 1 回も発生させない。他方、キャッシュミスヒット回数が最小の 1 の場合、動作エントリ数も 1 なので、キャッシュミスヒット発生部 314 は、不足エントリ数として、 $48 - 1 = 47$ を算出する。そして、47 回だけキャッシュミスヒットを発生させる。従って、最終的なキャッシュミスヒット回数の総数は $1 + 47 = 48$ となり、両者は均一化される。このため、第 2 の実施の形態と同様の理由で、キャッシュ攻撃型暗号解読法に対する防御が可能になる。

【0058】

以上の説明では、キャッシュ型攻撃暗号解読法で攻撃される可能性の高い換字テーブルについてだけ不足エントリ分のキャッシュミスヒットを発生させたが、全ての換字テーブルを対象にして同様のキャッシュミスヒットを発生させるようにしても良い。

【0059】

【発明の第 4 の実施の形態】

図 4 (a) を参照すると、本発明の第 4 の実施の形態にかかる暗号装置は、図 2 (a) の第 2 の実施の形態にかかる暗号装置と比較して、暗号プログラム 3 D に、使用エントリ管理部 312 および不使用エントリロード部 313 の代わりに、暗号処理または復号処理で換字テーブル 305 のエントリにキャッシュヒットした回数を管理する使用エントリ管理部 315 および前記キャッシュヒットした回数だけキャッシュミスヒットを発生させるキャッシュミスヒット発生部 316 とを備えている。ここで、使用エントリ管理部 315 とキャッシュミスヒット発生部 316 とで調整手段を構成する。以下、第 2 の実施の形態の暗号装置との相違

点を中心に、本実施の形態の構成と動作を説明する。

【0060】

図4（b）は使用エントリ管理部315に備わる管理テーブルの一例を示す。この管理テーブルは、キャッシュ攻撃型暗号解読法によって攻撃される可能性の高い換字テーブル毎に対応して設けられ、対応する換字テーブルと同数のエントリを持つ。管理テーブルの各エントリは、暗号処理および復号処理の開始時点で0の値にクリアされる。使用エントリ管理部315は、暗号処理または復号処理の過程で、攻撃される可能性の高い換字テーブルのエントリが参照される毎に、対応する管理テーブルの対応するエントリの値を+1する。

【0061】

キャッシュミスヒット発生部316は、実際の暗号処理または復号処理でもはや換字テーブル305が参照されなくなった時点で、図4（b）の管理テーブルを参照し、攻撃対象とされる可能性の高い換字テーブル毎に、キャッシュヒットした回数の総数を求め、その総数だけキャッシュミスヒットを発生させる。この処理は、第3の実施の形態のキャッシュミスヒット発生部314と同様に行える。

【0062】

次に本実施の形態の効果を説明する。今、攻撃対象とされる可能性の高い換字テーブルとして、MISTY1の換字テーブルS9を考える。この換字テーブルS9のエントリ総数は512、最大動作エントリ数は48である。図22で説明したように攻撃者は、暗号プログラム3Dの起動前に換字テーブルS9をクリアするため、1つの平文を暗号化する際の換字テーブルS9のキャッシュミスヒット回数の最大値は48である。また、最小数は第2の実施の形態と同様に1を想定する。

【0063】

キャッシュミスヒット回数が最大の48の場合、動作エントリ数も48なので、図4（b）の管理テーブルのエントリの値は、何れか48個のエントリだけが値1を示し、他の全てのエントリは値0になる。キャッシュミスヒット発生部316は、キャッシュヒット回数の総数として、2以上の値を持つエントリ毎に、そのエントリの値から1を引いた値を計算し、その結果を合計する。従って、今の

場合は0になる。従って、キャッシュミスヒット発生部316は1回もキャッシュミスヒットを発生させない。この結果、キャッシュミスヒット回数の総数は48となる。他方、キャッシュミスヒット回数が最小の1の場合、動作エントリ数も1なので、図4(b)の管理テーブルのエントリの値は、何れか1つのエントリの値が48になり、他の全てのエントリは値0になる。従って、キャッシュミスヒット発生部314は、キャッシュヒット回数として、 $48 - 1 = 47$ を求め、キャッシュミスヒットを47回発生させる。この結果、最終的なキャッシュミスヒット回数の総数は $1 + 47 = 48$ となり、両者は均一化される。このため、第2の実施の形態と同様の理由で、キャッシュ攻撃型暗号解読法に対する防御が可能になる。

【0064】

以上の説明では、キャッシュ型攻撃暗号解読法で攻撃される可能性の高い換字テーブルについてだけキャッシュヒット回数分のキャッシュミスヒットを発生させたが、全ての換字テーブルを対象にして同様のキャッシュミスヒットを発生させるようにしても良い。

【0065】

また、本実施の形態では、キャッシュヒットした回数分のキャッシュミスヒットをキャッシュミスヒット発生部316でまとめて発生したが、他の実施の形態として、使用エントリ管理部315にキャッシュミスヒットを発生させる機能を持たせ、キャッシュヒットが発生する毎に、つまり図4(b)の管理テーブルの或るエントリの値を+1したときに2以上の値となる毎に、1回だけキャッシュミスヒットを発生させるようにしても良い。

【0066】

【発明の第5の実施の形態】

図5を参照すると、本発明の第5の実施の形態にかかる暗号装置は、図14に示した従来の暗号装置と比較して、暗号プログラム3Eは、換字テーブル305が1つの平文または1つの暗号文の暗号処理または復号処理でn回参照される場合に、換字テーブル305と同じ内容を持つn個の換字テーブル305-1～305-nを備え、データ変換部304は、1つの平文または1つの暗号文の暗号処

理または復号処理において換字テーブル 305 を参照する場合、各参照毎にそれぞれ異なる換字テーブル 305-1 ~ 305-n を参照するように構成される点で相違する。

【0067】

この第5の実施の形態によれば、1つの平文または1つの暗号文の暗号処理または復号処理において、データ変換部 304 は、換字テーブル 305 を参照する場合、各参照毎にそれぞれ異なる換字テーブル 305-1 ~ 305-n を参照するため、何回必ずキャッシュミスヒットが発生する。このため、任意の平文または暗号文について、換字テーブルに対するキャッシュミスヒット回数を均一化することができる。従って、キャッシュ攻撃型暗号解読法による攻撃を防御することができる。

【0068】

同じ内容の換字テーブルを n 個独立して備えるようにする換字テーブルは、キャッシュ型攻撃暗号解読法で攻撃される可能性の高い換字テーブルのみとする構成以外に、全ての換字テーブルを対象に複数備える構成が考えられる。

【0069】

【発明の第6の実施の形態】

図6を参照すると、本発明の第6の実施の形態にかかる暗号装置は、図14の従来の暗号装置と比較して、暗号プログラム 3F に、暗号処理および復号処理の開始時に内部のタイマ T を起動するタイマ起動部 321 と、暗号処理および復号処理の終了時にタイマ T のタイマ値が予め設定された暗号処理または復号処理の最大時間 T_{max} より短いかどうかを判定する判定部 322 と、タイマ T のタイマ値が最大時間 T_{max} より短い場合に、その差の時間「 $T_{max} - T$ 」だけ暗号処理または復号処理の時間を延長するためにウェイトを行うウェイト部 323 とを備えている。ここで、タイマ起動部 321 と判定部 322 とウェイト部 323 とで調整手段を構成する。

【0070】

上記の最大時間 T_{max} としては、例えば、図19に示したような暗号化時間分布における最大の暗号化時間が用いられる。勿論、その最大の暗号化時間より若干

長い時間を設定しても良い。

【0071】

本実施の形態の暗号装置によれば、1つの平文または1つの暗号文の暗号処理または復号処理における暗号処理時間および復号処理時間が、任意の平文または暗号文についてほぼ均一化するため、図19の暗号化時間分布が最大の暗号化時間の箇所に集中する。このため、キャッシュ攻撃型暗号解読法による攻撃を防御することができる。

【0072】

【発明の第7の実施の形態】

図7を参照すると、本発明の第7の実施の形態にかかる暗号装置は、図6の第6の実施の形態の暗号装置と比較して、暗号プログラム3Gに、ウエイト部323に代えて、予め定められた一定時間 T_c だけウエイトを行うウエイト部324を備えている。ここで、一定時間 T_c としては、例えば、図19に示したような暗号化時間分布における最大暗号時間の半分の時間を用いる。勿論、それより若干長い時間、短い時間を設定しても良い。ここで、タイマ起動部321と判定部322とウエイト部324とで調整手段を構成する。

【0073】

本実施の形態の暗号装置によれば、図19に示した暗号化時間分布の中央部分の山が最大の暗号時間の箇所に移動し、真に最大暗号時間を与えた平文に混合される。このため、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【0074】

【発明の第8の実施の形態】

図8を参照すると、本発明の第8の実施の形態にかかる暗号装置は、図7の第7の実施の形態の暗号装置と比較して、暗号プログラム3Hに、ウエイト部324に代えて、0か1の何れかの値をとる乱数 r を無作為に生成する乱数生成部325、生成した乱数 r が0か否かを判定する判定部326、乱数 r が0の場合に、ウエイト時間 t を乱数によって生成するウエイト時間生成部327、生成された

ウェイト時間 t だけウェイトを行うウェイト部 328 を備えている。ここで、タイマ起動部 321 と判定部 322、326 と、乱数生成部 325 とウェイト時間生成部 327 とウェイト部 328 とで調整手段を構成する。ウェイト時間生成部 327 は、図 19 に示したような暗号化時間分布におけるほぼ最大暗号時間から時間 0 の範囲内で、ウェイト時間 t を無作為に生成する。

【0075】

本実施の形態の暗号装置によれば、図 19 に示した暗号化時間分布の特性が不定なものとなり、真に最大暗号時間を与えた平文とそれ以外の平文とが同じ暗号時間帯に出現する。このため、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となり、その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【0076】

【発明の第 9 の実施の形態】

図 9 を参照すると、本発明の第 9 の実施の形態にかかる暗号装置は、図 14 の従来の暗号装置と比較して、暗号プログラム 3 I に、0 か 1 の何れかの値をとる乱数 r を無作為に生成する乱数生成部 331、生成した乱数 r が 0 か否かを判定する判定部 332、乱数 r が 0 の場合に、予め定められた一定時間 T_c だけウェイトを行うウェイト部 333 を備えている。ここで、乱数生成部 331 と判定部 332 とウェイト部 333 とで調整手段を構成する。一定時間 T_c としては、例えば、図 19 に示したような暗号化時間分布における最大暗号時間の半分の時間を用いる。勿論、それより若干長い時間、短い時間を設定しても良い。

【0077】

本実施の形態の暗号装置によれば、図 19 に示した暗号化時間分布の特性が不定なものとなり、真に最大暗号時間を与えた平文は同じ暗号時間に揃わず、また、それ以外の平文と同じ暗号時間帯に出現する。このため、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となり、その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【0078】

なお、図 9 の実施の形態では、暗号プログラム 3 I の終了間際でウェイトを行う

ようにしているが、ウエイトする箇所は暗号プログラム 3 I の任意の箇所で良い。また、複数の箇所で分散的にウエイトするようにしても良い。

【0079】

【発明の第10の実施の形態】

図10を参照すると、本発明の第10の実施の形態にかかる暗号装置は、図14の従来の暗号装置と比較して、暗号プログラム 3 J に、ウエイト時間 t を乱数によって生成するウエイト時間生成部 334、生成されたウエイト時間 t だけウエイトを行うウエイト部 335 を備えている。ここで、ウエイト時間生成部 334 とウエイト部 335 とで調整手段を構成する。ウエイト時間生成部 334 は、図19に示したような暗号化時間分布におけるほぼ最大暗号時間から時間0の範囲内で、ウエイト時間 t を無作為に生成する。

【0080】

本実施の形態の暗号装置によれば、図19に示した暗号化時間分布の特性が不定なものとなり、真に最大暗号時間を与えた平文は同じ暗号時間に揃わず、また、それ以外の平文と同じ暗号時間帯に出現する。このため、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となり、その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【0081】

なお、図10の実施の形態では、暗号プログラム 3 J の終了間際でウエイトを行うようにしているが、ウエイトする箇所は暗号プログラム 3 J の任意の箇所で良い。また、複数の箇所で分散的にウエイトするようにしても良い。

【0082】

【発明の第11の実施の形態】

図11を参照すると、本発明の第11の実施の形態にかかる暗号装置は、図10の第10の実施の形態の暗号装置と比較して、暗号プログラム 3 K に、0か1の何れかの値をとる乱数 r を無作為に生成する乱数生成部 336 と生成した乱数 r が0か否かを判定する判定部 337 とが追加され、ウエイト時間 t を乱数によって生成するウエイト時間生成部 334 および生成されたウエイト時間 t だけウエイトを行うウエイト部 335 は、0の乱数 r が生成された場合に限って動作する

。ここで、乱数生成部 336 と判定部 337 とウエイト時間生成部 334 とウエイト部 335 とで調整手段を構成する。ウエイト時間生成部 334 が生成するウエイト時間 t は、例えば、図 19 に示したような暗号化時間分布におけるほぼ最大暗号時間から時間 0 の範囲内で無作為に生成される。

【0083】

本実施の形態の暗号装置によれば、図 19 に示した暗号化時間分布の特性が不定なものとなり、真に最大暗号時間を与えた平文は同じ暗号時間に揃わず、また、それ以外の平文と同じ暗号時間帯に出現する。このため、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となり、その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【0084】

なお、図 11 の実施の形態では、暗号プログラム 3K の終了間際でウエイトを行うようにしているが、ウエイトする箇所は暗号プログラム 3K の任意の箇所で良い。また、複数の箇所で分散的にウエイトするようにしても良い。

【0085】

【発明の第 12 の実施の形態】

図 12 を参照すると、本発明の第 12 の実施の形態にかかる暗号装置は、図 14 の従来の暗号装置と比較して、暗号プログラム 3L が、換字処理に用いる換字テーブルのうち攻撃対象とされる可能性の高い換字テーブル以外はテーブル構造の換字テーブルとして備えるが、攻撃対象とされる可能性の高い換字テーブルは持たず、演算処理によって等価な換字処理を実行する点で相違する。換字テーブルを使わずに等価な換字処理を実現する演算処理の一例としてブール演算を使う方法が考えられる。以下、2 ビットの例で説明する。今、(0, 1, 2, 3) を (3, 0, 1, 2) に変換するものとする。入力 of 各ビットを x_1 、 x_2 、出力の各ビットを y_1 、 y_2 とすると、以下のように表現される。

$$\begin{aligned} & ((x_1 x_2), (x_1 x_2), (x_1 x_2), (x_1 x_2)) \\ &= ((0 \ 0), (0 \ 1), (1 \ 0), (1 \ 1)) \\ &\rightarrow ((y_1 y_2), (y_1 y_2), (y_1 y_2), (y_1 y_2)) \\ &= ((1 \ 1), (0 \ 0), (0 \ 1), (1 \ 0)) \end{aligned}$$

ここで、 x_1 と x_2 の排他的論理和をとると(0, 1, 1, 0)なので、この排他的論理和を反転(not)すると(1, 0, 0, 1)となり、 y_1 の列(1, 0, 0, 1)と等しくなる。また、 y_2 の列(1, 0, 1, 0)は x_2 の列(0, 1, 0, 1)を反転したものに等しい。従って、(0, 1, 2, 3)を(3, 0, 1, 2)に変換する演算処理は、以下のブール式で実現できる。

$$y_1 = \neg (x_1 \circ x_2)$$

$$y_2 = \neg x_2$$

… (3)

ここで、 \neg は反転(not)、 \circ は排他的論理和を示す。

【0086】

本実施の形態の暗号装置によれば、キャッシュ型攻撃暗号解読法による攻撃の可能性の高い換字テーブルを使わないので、それに対するキャッシュミスはそもそも発生せず、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。その結果、鍵差分を決定できず、結果として鍵の解読が困難となる。

【0087】

本実施の形態では、攻撃対象となる可能性の高い換字テーブルだけを無くしたが、攻撃対象となる可能性の低い換字テーブルも無くして、演算処理によって等価な換字処理を実行するようにしても良い。

【0088】

【発明の効果】

以上説明したように本発明によれば、キャッシュ攻撃型暗号解読法という新たな暗号解読法による攻撃によって秘密鍵を推測されることを防止することができるという効果が得られる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態にかかる暗号装置の構成図である。

【図2】

本発明の第2の実施の形態にかかる暗号装置の構成図である。

【図 3】

本発明の第 3 の実施の形態にかかる暗号装置の構成図である。

【図 4】

本発明の第 4 の実施の形態にかかる暗号装置の構成図である。

【図 5】

本発明の第 5 の実施の形態にかかる暗号装置の構成図である。

【図 6】

本発明の第 6 の実施の形態にかかる暗号装置の構成図である。

【図 7】

本発明の第 7 の実施の形態にかかる暗号装置の構成図である。

【図 8】

本発明の第 8 の実施の形態にかかる暗号装置の構成図である。

【図 9】

本発明の第 9 の実施の形態にかかる暗号装置の構成図である。

【図 1 0】

本発明の第 1 0 の実施の形態にかかる暗号装置の構成図である。

【図 1 1】

本発明の第 1 1 の実施の形態にかかる暗号装置の構成図である。

【図 1 2】

本発明の第 1 2 の実施の形態にかかる暗号装置の構成図である。

【図 1 3】

換字テーブルの構成例を示す図である。

【図 1 4】

従来の暗号装置の構成図である。

【図 1 5】

キャッシュ攻撃型暗号解読法の原理説明図である。

【図 1 6】

キャッシュ攻撃型暗号解読法による鍵差分値の決定方法の説明図である。

【図 1 7】

MISTY1 のデータランダム化部の構成を示す図である。

【図 1 8】

MISTY1 のデータランダム化部で使用される FO_i 関数と、さらにこの FO_i 関数で使用する FI_{ij} 関数の構成を示す図である。

【図 1 9】

暗号化時間分布を示す図である。

【図 2 0】

MISTY1 で使われる換字テーブル S9 の動作エントリ数と暗号化時間との関係を示す図である。

【図 2 1】

MISTY1 で使われる換字テーブル S7 の動作エントリ数と暗号化時間との関係を示す図である。

【図 2 2】

暗号過程で換字テーブル S9 の全エントリがほぼ参照される可能性の高い平文の集合を抽出する処理例を示すフローチャートである。

【符号の説明】

1…CPU

2…メモリ（主記憶）

3、3A～3L…暗号プログラム

4…キャッシュ

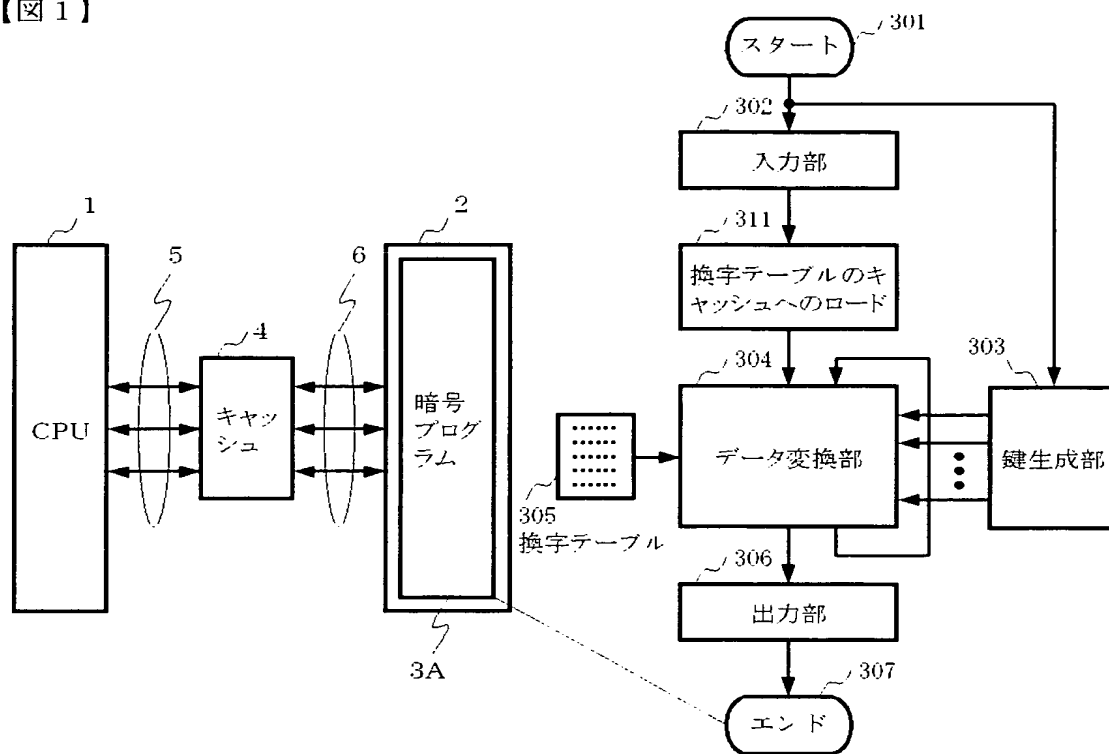
5…プロセッサバス

6…メモリバス

【書類名】 図面

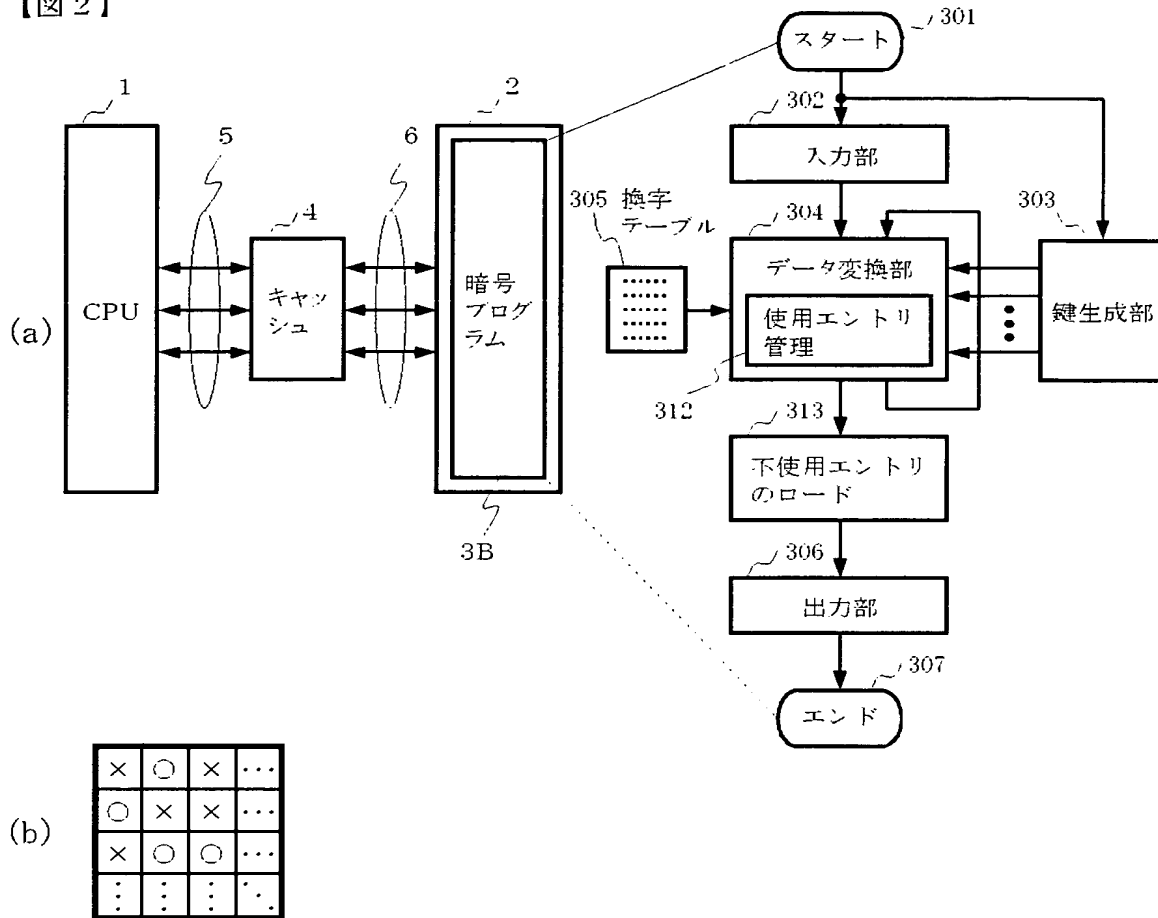
【図 1】

【図 1】



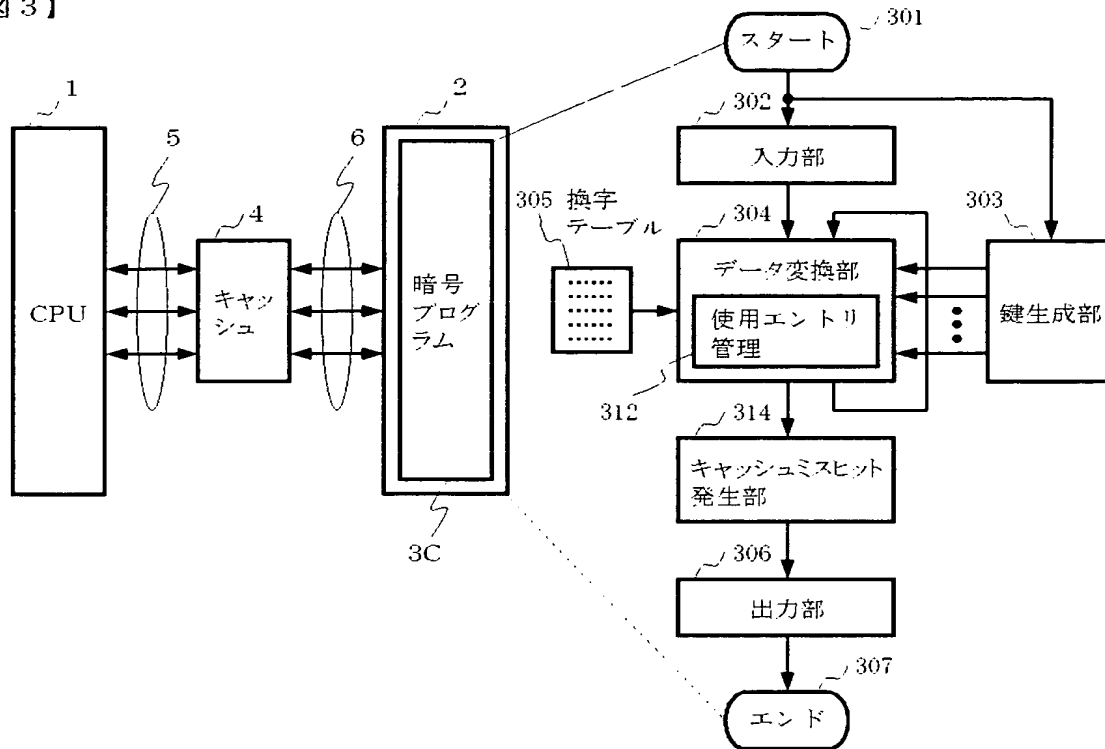
【図 2】

【図 2】



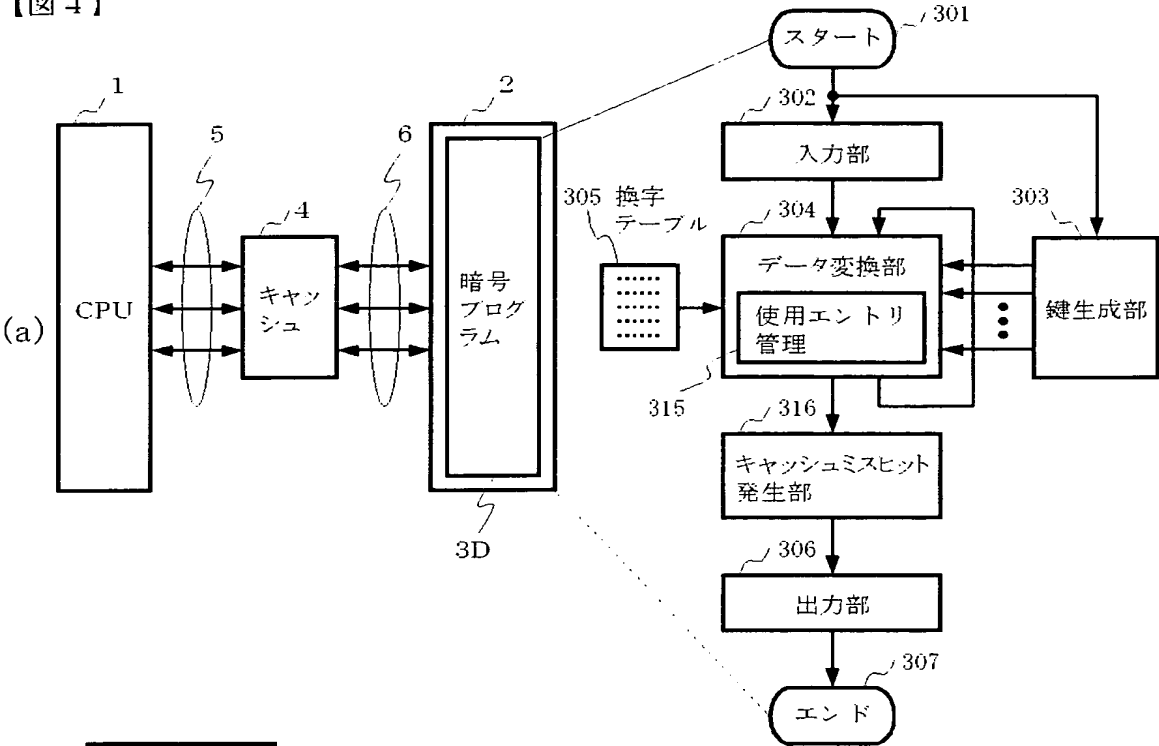
【図 3】

【図 3】



【図 4】

【図 4】

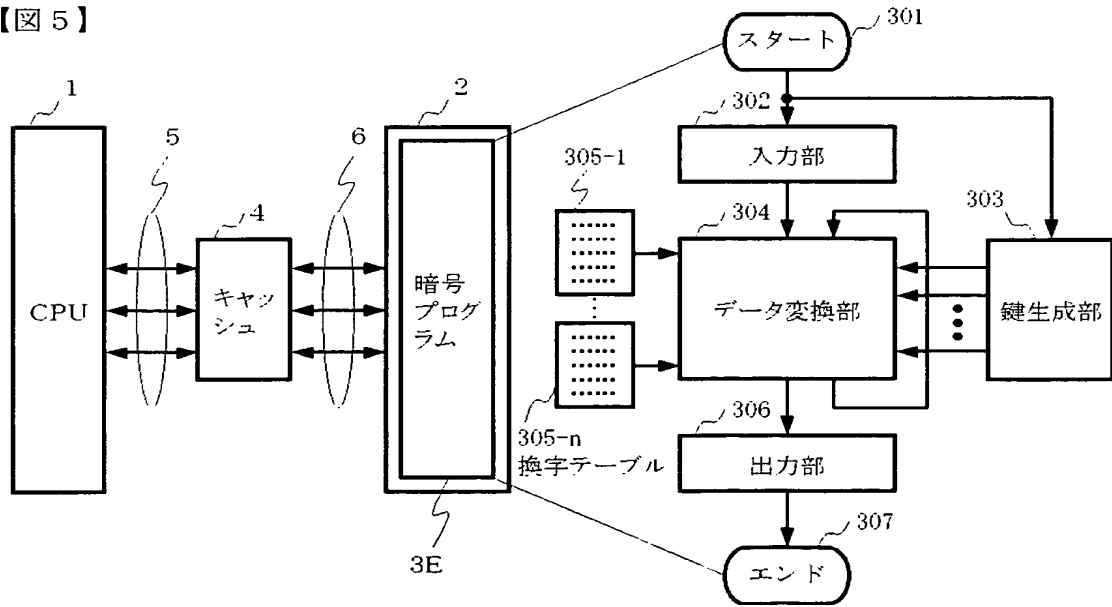


(b)

0	2	0	...
1	0	0	...
0	1	2	...
⋮	⋮	⋮	⋮

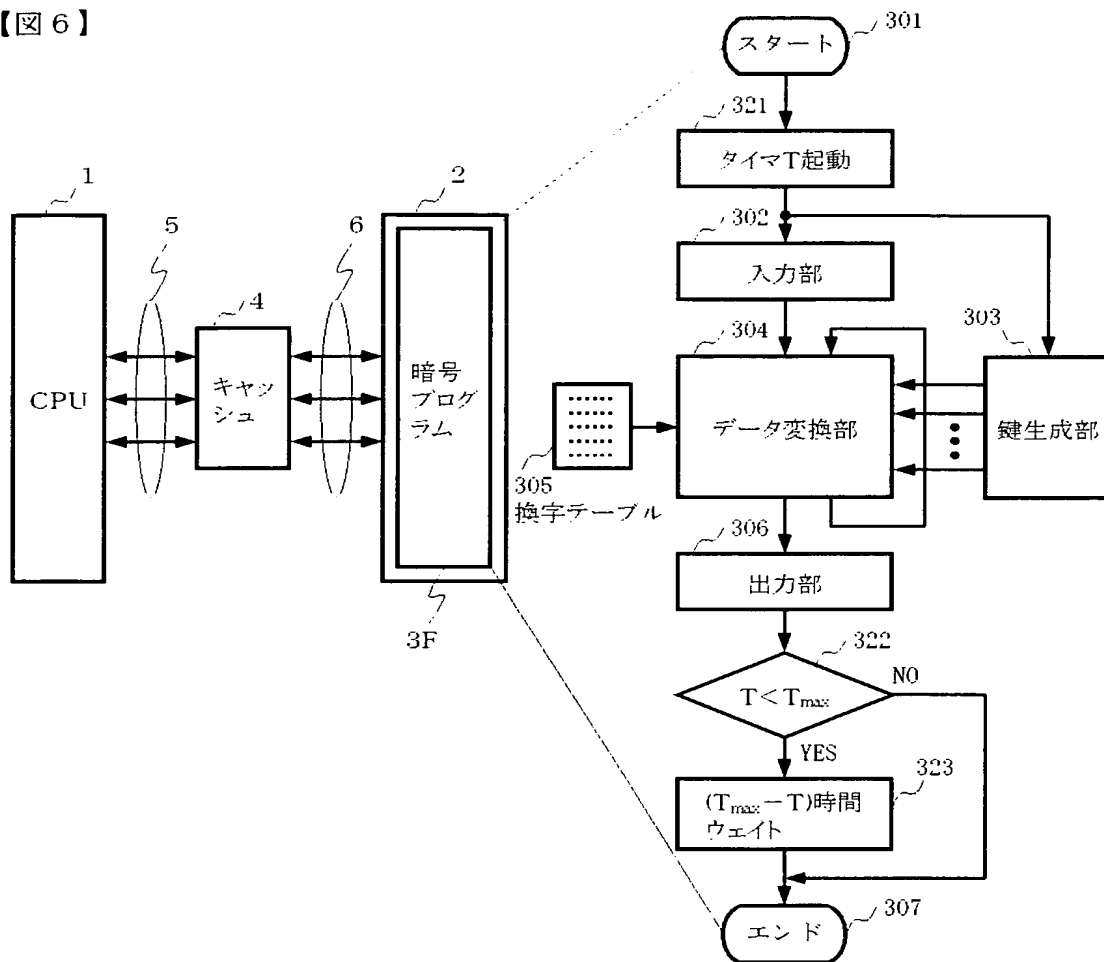
【図 5】

【図 5】



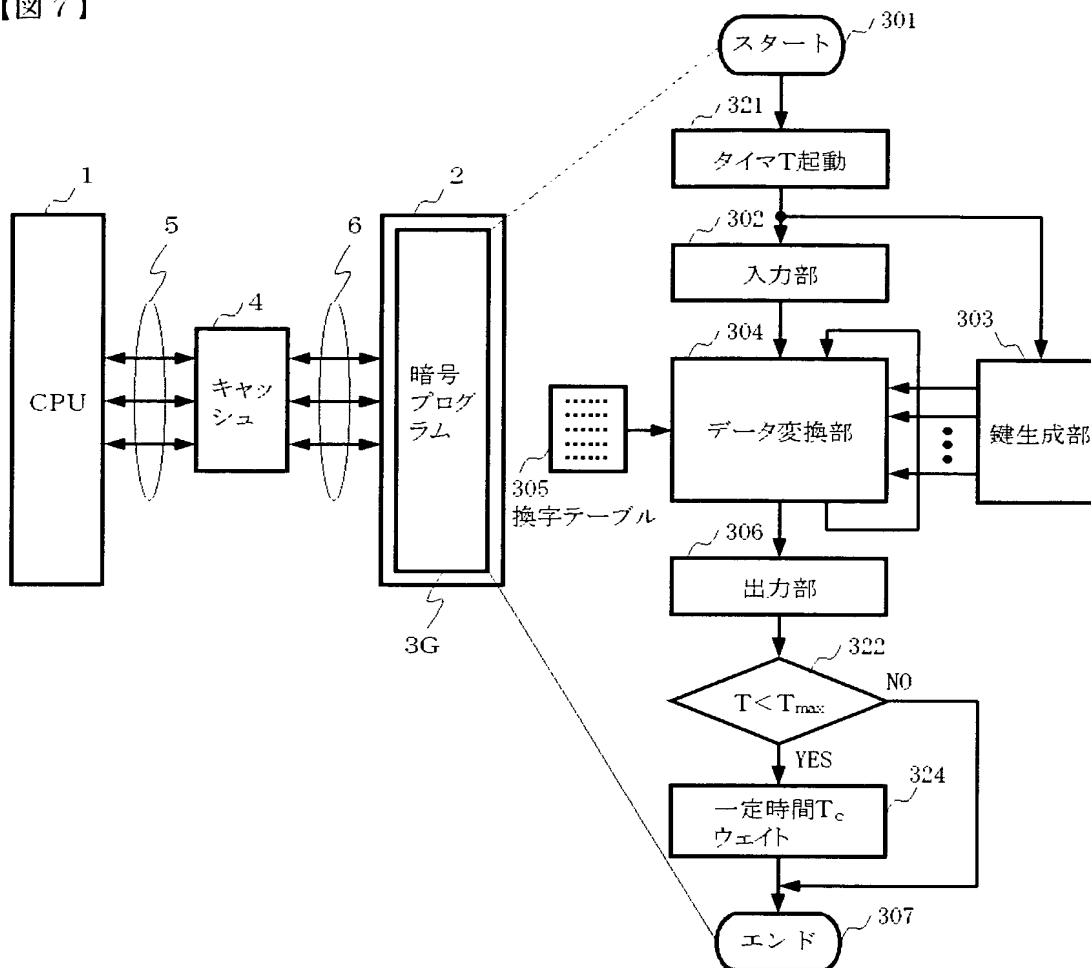
【図 6】

【図 6】



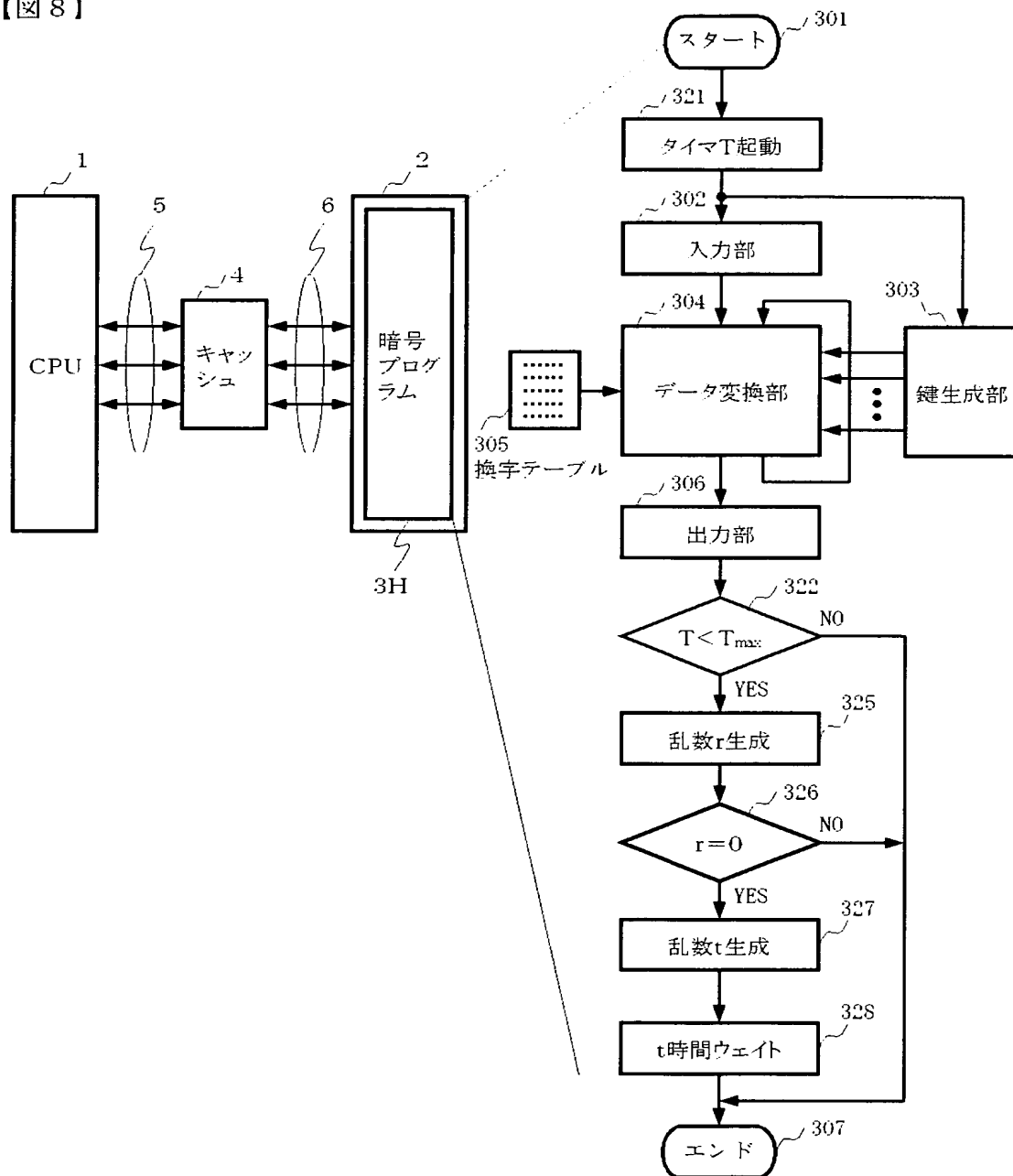
【図 7】

【図 7】



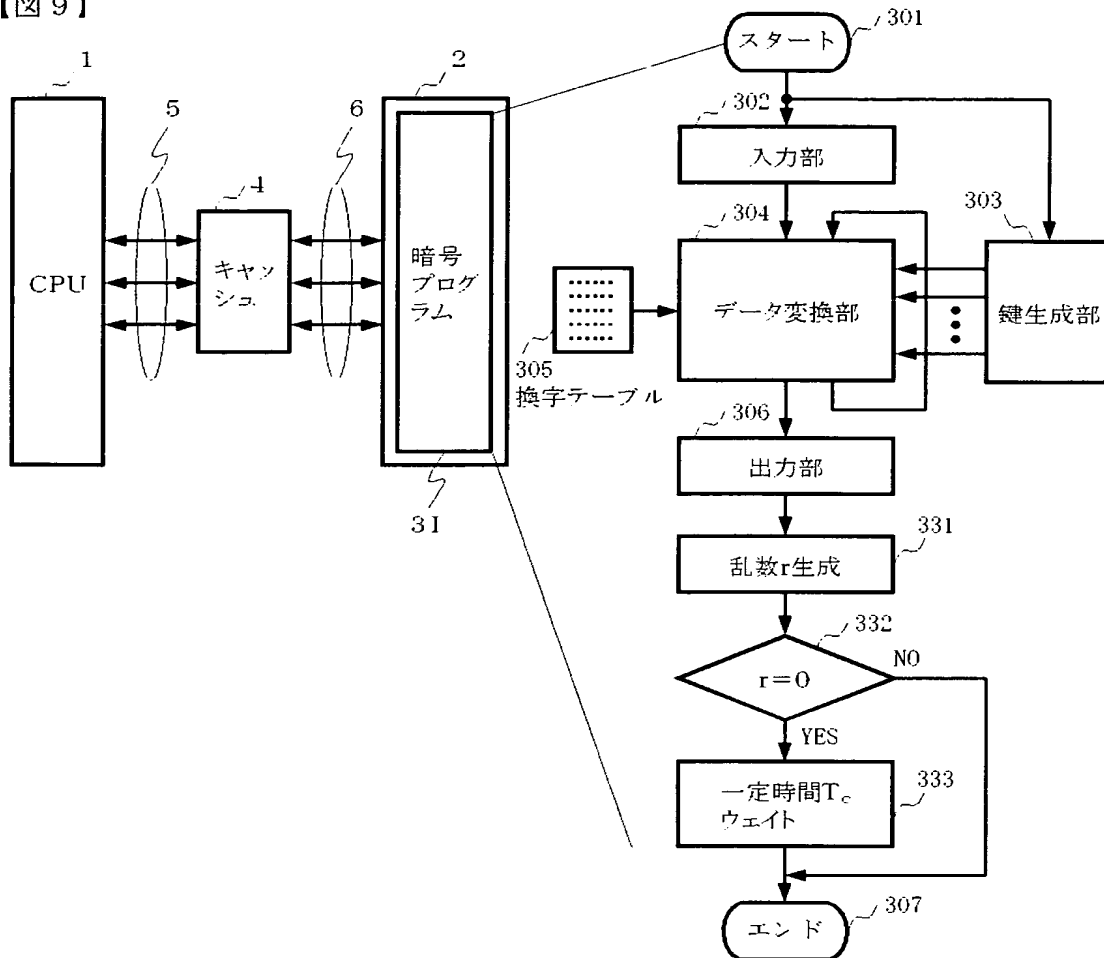
【図 8】

【図 8】



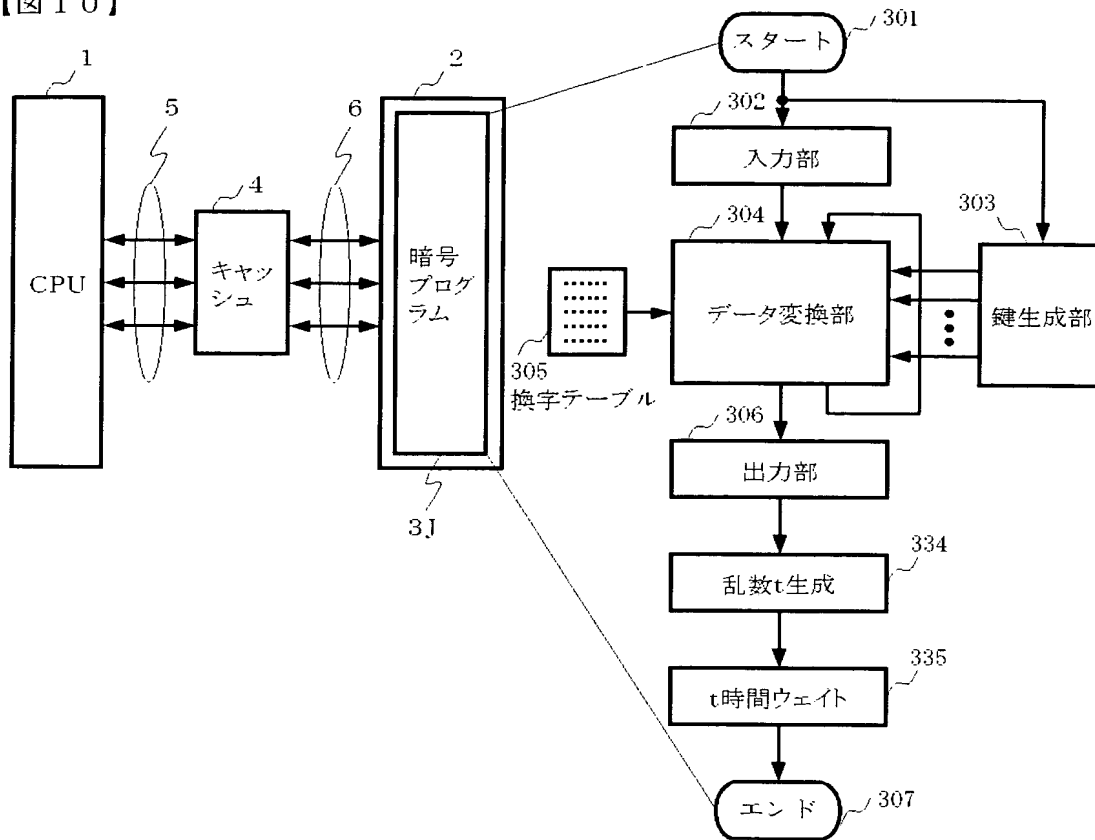
【図 9】

【図 9】



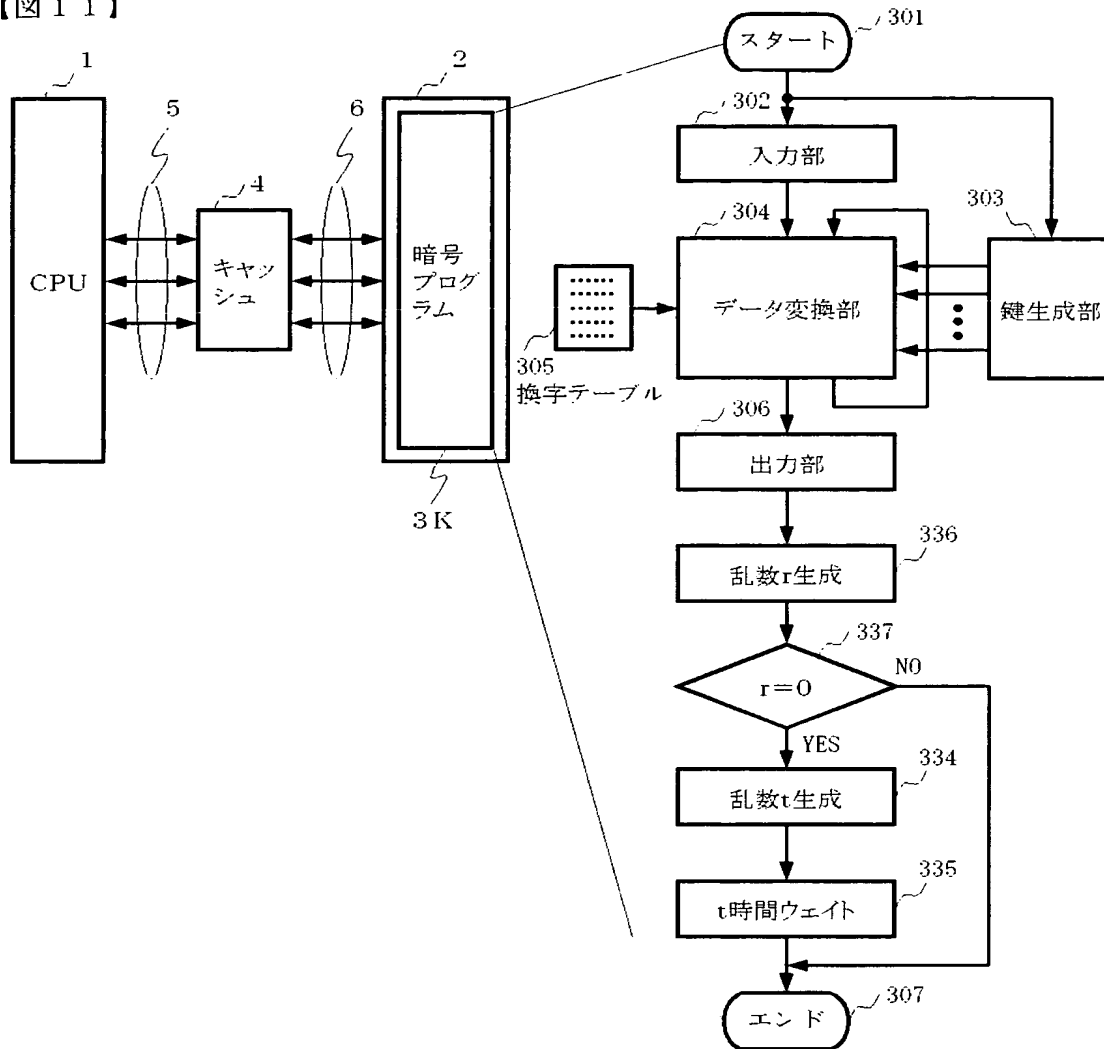
【図 10】

【図 10】



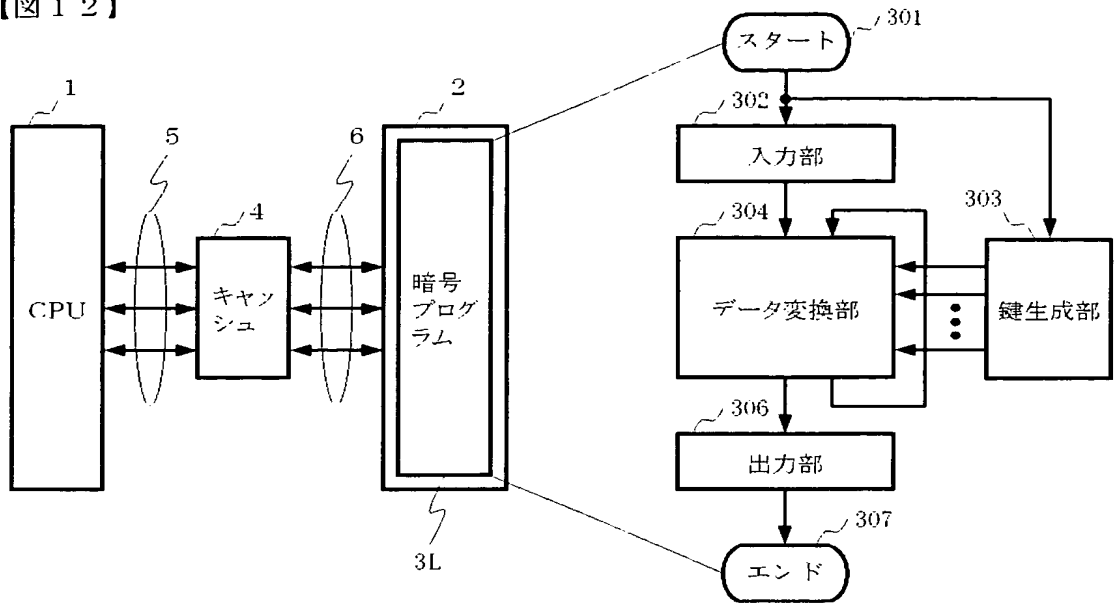
【図 11】

【図 11】



【図 1 2】

【図 1 2】



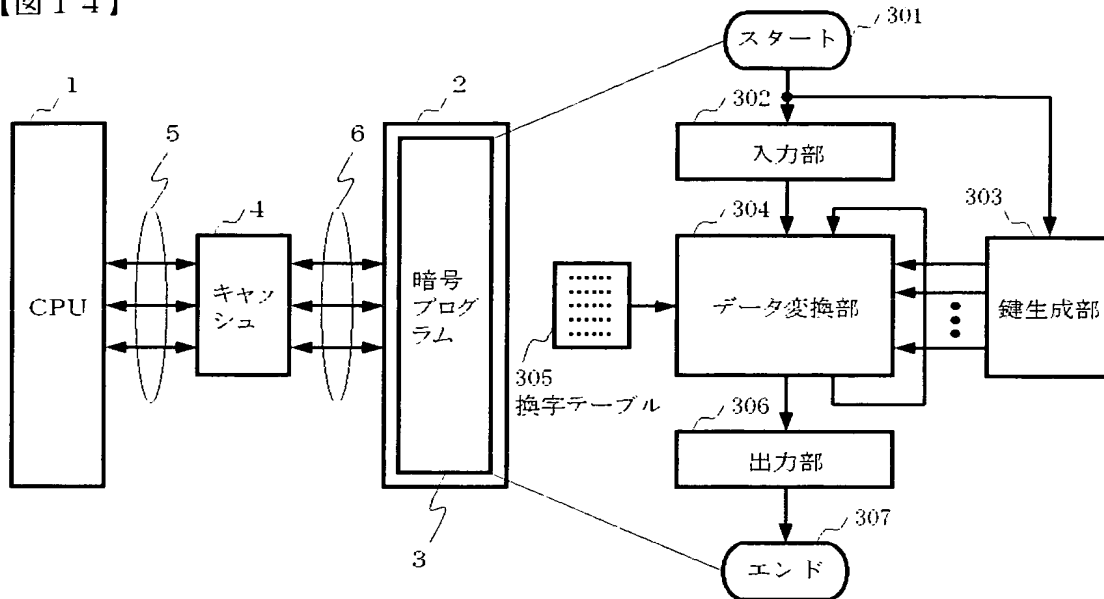
【図 1 3】

【図 1 3】

8	1	3	F
A	6	C	5
4	9	0	E
B	2	7	D

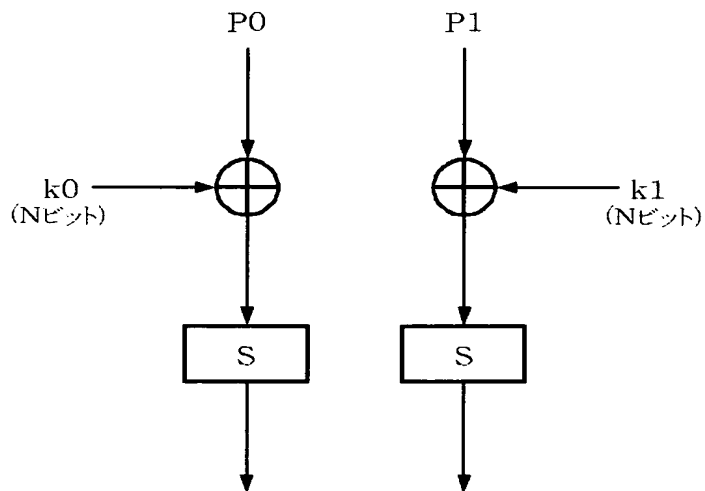
【図 14】

【図 14】



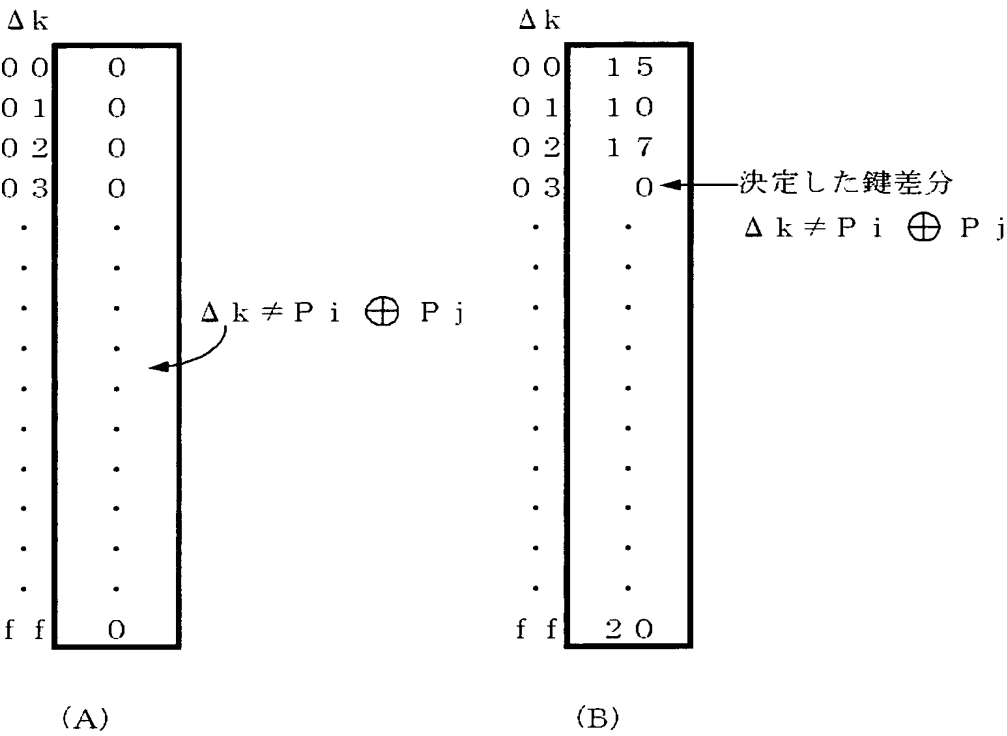
【図 15】

【図 15】



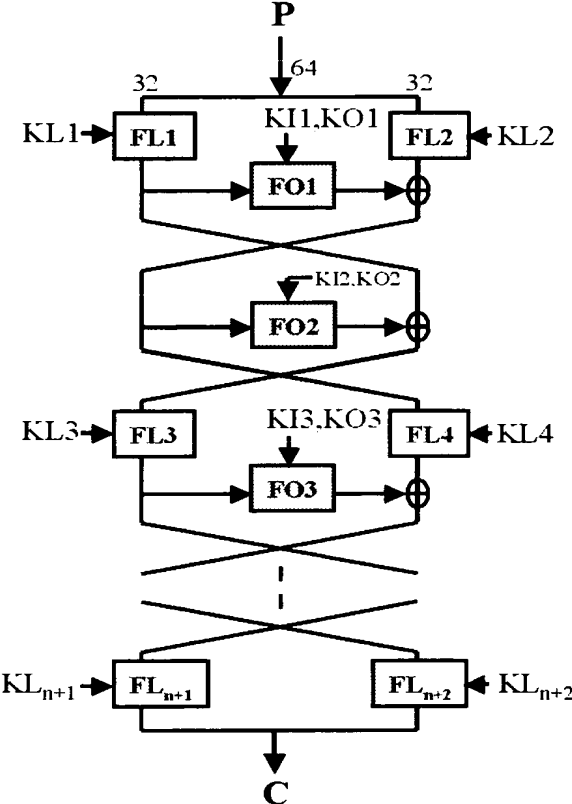
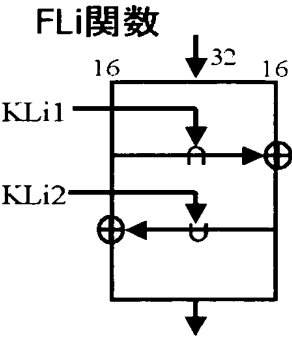
【図 1 6】

【図 1 6】



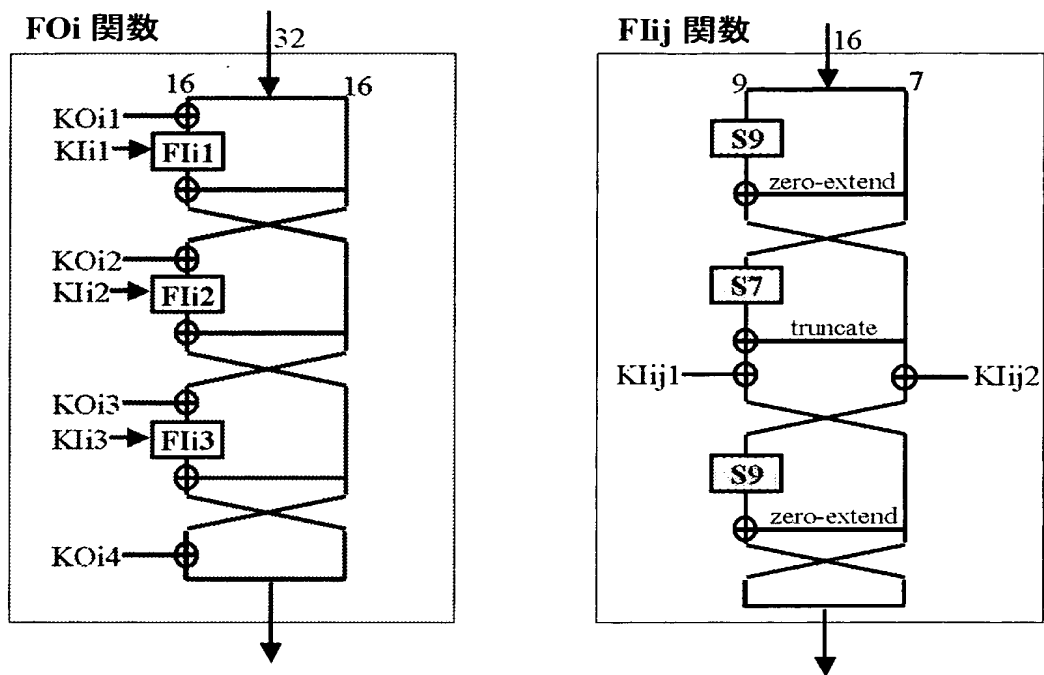
【図 1 7】

【図 1 7】



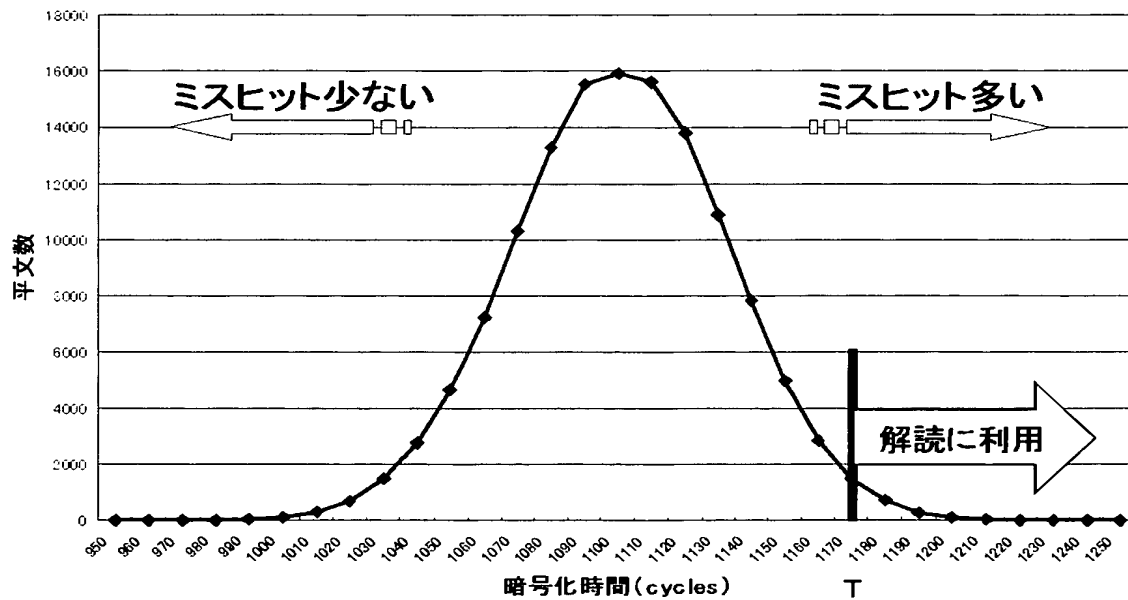
【図 18】

【図 18】



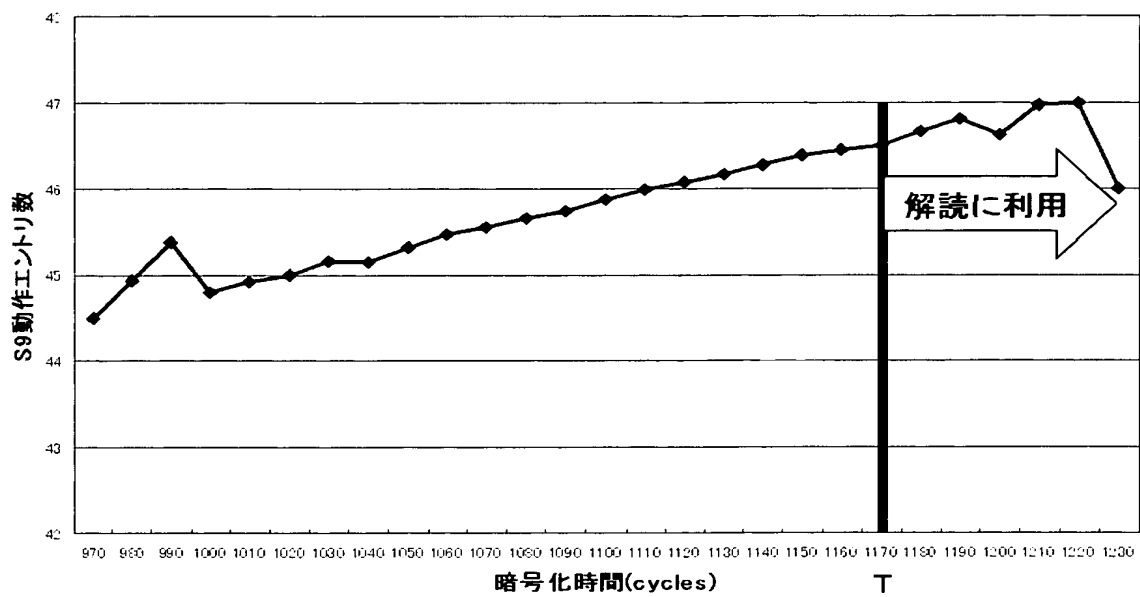
【図 19】

【図 19】



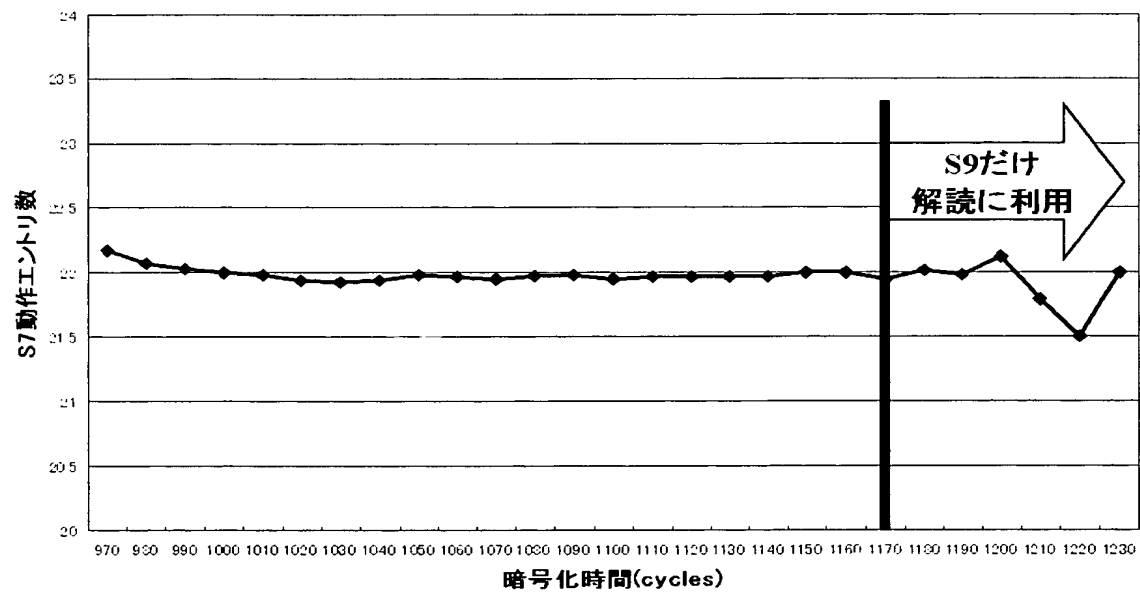
【図 20】

【図 20】



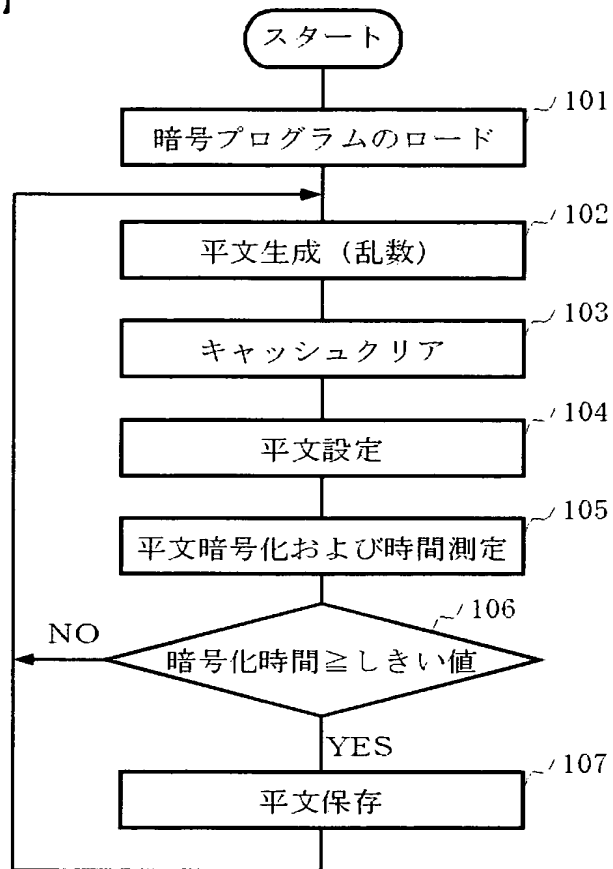
【図 21】

【図 21】



【図 22】

【図 22】



【書類名】 要約書

【要約】

【課題】 キャッシュ攻撃型暗号解読法という新たな暗号解読法に対する防御機能を備えた暗号装置を提供する。

【解決手段】 ビット列変換に使用する換字テーブル 3 0 5 を用いて暗号処理を行う暗号プログラム 3 A がキャッシュ 4 を有するコンピュータに実装された暗号装置において、暗号処理に先立って換字テーブル 3 0 5 をキャッシュ 4 にプリロードする手段 3 1 1 を備える。1 つの平文の暗号処理における換字テーブル 3 0 5 に対するアクセス時のキャッシュミスヒット回数が、任意の平文についてほぼ均一化されるため、換字テーブルの動作エントリ数が少ない平文も多い平文も、その暗号時間がほぼ同じになり、キャッシュ型攻撃暗号解読法の要である鍵差分を抽出する際に用いる平文の抽出が困難となる。

【選択図】 図 1

特願 2 0 0 2 - 2 8 0 4 6 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社